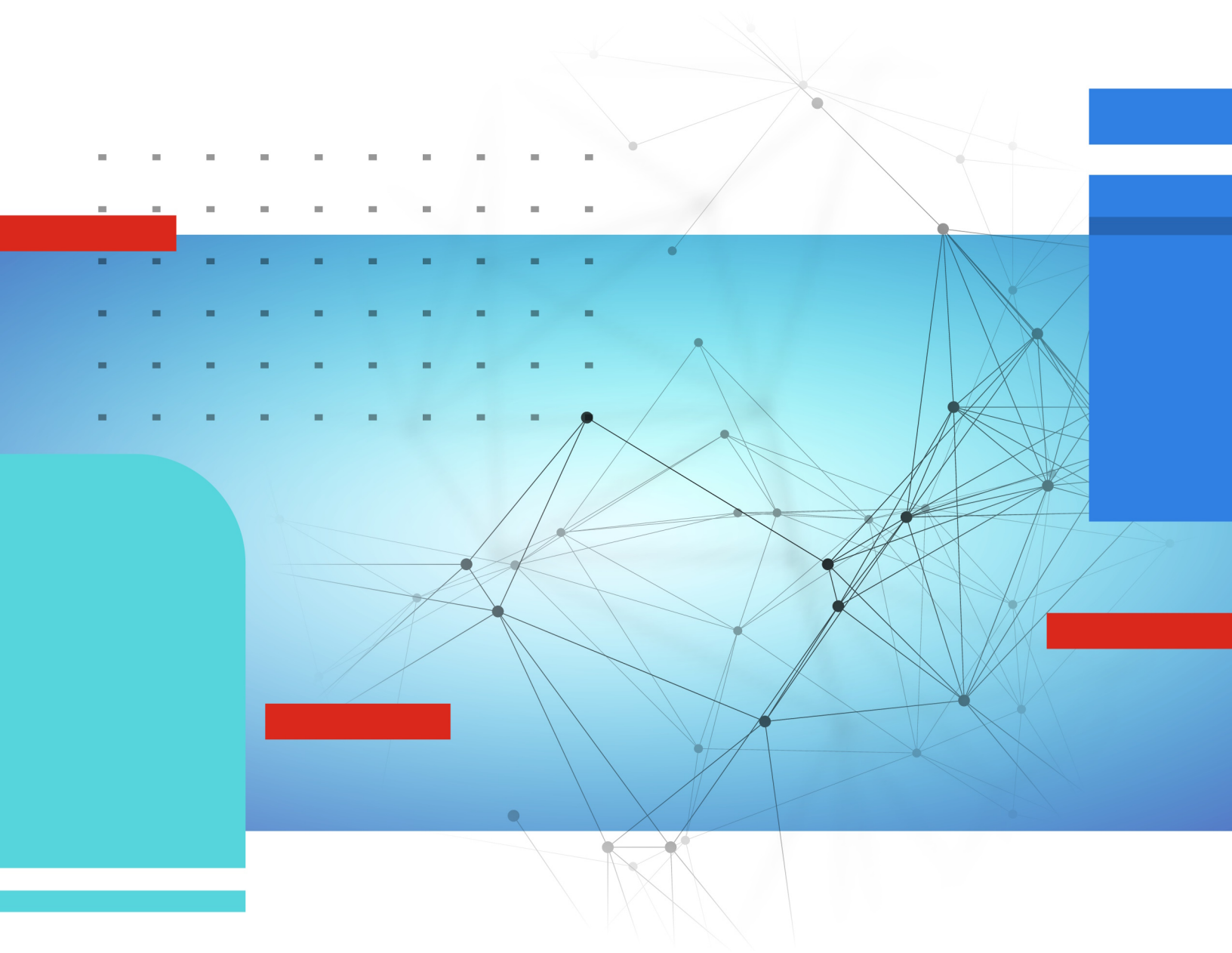




CLI Reference

FortiOS 7.6.3



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



April 16, 2025

FortiOS 7.6.3 CLI Reference

01-763-1048597-20250416

TABLE OF CONTENTS

Change Log	110
FortiOS CLI reference	111
Availability of commands and options	111
Command tree	111
CLI configuration commands	113
alertemail	114
config alertemail setting	114
antivirus	121
config antivirus exempt-list	121
config antivirus profile	122
config antivirus quarantine	155
config antivirus settings	159
application	161
config application custom	161
config application group	162
config application list	163
config application name	172
config application rule-settings	174
authentication	175
config authentication rule	175
config authentication scheme	178
config authentication setting	180
automation	184
config automation setting	184
aws	185
config aws vpce	185
azure	187
config azure migration	187
config azure nva	188
config azure vwan-ingress-public-IPs	189
config azure vwan-slb	190
casb	194
config casb attribute-match	194
config casb profile	196
config casb saas-application	201
config casb user-activity	204
certificate	212
config certificate ca	212
config certificate crl	214
config certificate hsm-local	215
config certificate local	219
config certificate remote	224
diameter-filter	226
config diameter-filter profile	226

dlp	229
config dlp data-type	229
config dlp dictionary	231
config dlp exact-data-match	233
config dlp filepattern	234
config dlp fp-doc-source	238
config dlp label	241
config dlp profile	242
config dlp sensitivity	248
config dlp sensor	248
config dlp settings	250
dnsfilter	252
config dnsfilter domain-filter	252
config dnsfilter profile	253
dpdk	260
config dpdk cpus	260
config dpdk global	262
emailfilter	265
config emailfilter block-allow-list	265
config emailfilter bword	267
config emailfilter dnsbl	269
config emailfilter fortishield	270
config emailfilter iptrust	271
config emailfilter mheader	272
config emailfilter options	274
config emailfilter profile	274
endpoint-control	283
config endpoint-control fctems	283
config endpoint-control fctems-override	287
config endpoint-control settings	291
ethernet-oam	293
config ethernet-oam cfm	293
extension-controller	296
config extension-controller dataplan	296
config extension-controller extender	299
config extension-controller extender-profile	303
config extension-controller extender-vap	333
config extension-controller fortigate	336
config extension-controller fortigate-profile	338
file-filter	340
config file-filter profile	340
firewall	343
config firewall DoS-policy	345
config firewall DoS-policy6	348
config firewall access-proxy	350
config firewall access-proxy6	386
config firewall access-proxy-ssh-client-cert	422
config firewall access-proxy-virtual-host	424

config firewall acl	426
config firewall acl6	428
config firewall address	429
config firewall address6	435
config firewall address6-template	440
config firewall addrgrp	442
config firewall addrgrp6	444
config firewall auth-portal	446
config firewall central-snat-map	446
config firewall city	449
config firewall country	450
config firewall decrypted-traffic-mirror	451
config firewall dnstranslation	451
config firewall global	452
config firewall identity-based-route	453
config firewall interface-policy	454
config firewall interface-policy6	457
config firewall internet-service	461
config firewall internet-service-addition	463
config firewall internet-service-append	464
config firewall internet-service-botnet	465
config firewall internet-service-custom	465
config firewall internet-service-custom-group	467
config firewall internet-service-definition	468
config firewall internet-service-extension	469
config firewall internet-service-group	473
config firewall internet-service-ipbl-reason	474
config firewall internet-service-ipbl-vendor	474
config firewall internet-service-list	475
config firewall internet-service-name	475
config firewall internet-service-owner	476
config firewall internet-service-reputation	477
config firewall internet-service-sld	477
config firewall internet-service-subapp	478
config firewall ipmacbinding setting	479
config firewall ipmacbinding table	479
config firewall ippool	480
config firewall ippool6	486
config firewall ipv6-eh-filter	487
config firewall ip-translation	489
config firewall ldb-monitor	490
config firewall local-in-policy	492
config firewall local-in-policy6	495
config firewall multicast-address	499
config firewall multicast-address6	500
config firewall multicast-policy	501
config firewall multicast-policy6	504
config firewall network-service-dynamic	506
config firewall on-demand-sniffer	507

config firewall policy	508
config firewall profile-group	534
config firewall profile-protocol-options	536
config firewall proxy-address	561
config firewall proxy-addrgrp	566
config firewall proxy-policy	567
config firewall region	577
config firewall schedule group	578
config firewall schedule onetime	579
config firewall schedule recurring	580
config firewall security-policy	581
config firewall service category	591
config firewall service custom	592
config firewall service group	596
config firewall shaper per-ip-shaper	597
config firewall shaper traffic-shaper	599
config firewall shaping-policy	602
config firewall shaping-profile	607
config firewall sniffer	610
config firewall ssh host-key	615
config firewall ssh local-ca	617
config firewall ssh local-key	618
config firewall ssh setting	619
config firewall ssl setting	620
config firewall ssl-server	622
config firewall ssl-ssh-profile	625
config firewall traffic-class	656
config firewall ttl-policy	656
config firewall vendor-mac	657
config firewall vip	658
config firewall vip6	695
config firewall vipgrp	729
config firewall vipgrp6	729
config firewall wildcard-fqdn custom	730
config firewall wildcard-fqdn group	731
ftp-proxy	733
config ftp-proxy explicit	733
icap	736
config icap profile	736
config icap server	743
config icap server-group	744
ips	746
config ips custom	746
config ips decoder	748
config ips global	748
config ips rule	753
config ips rule-settings	755
config ips sensor	755
config ips settings	761

config ips view-map	762
log	764
config log azure-security-center filter	766
config log azure-security-center setting	770
config log azure-security-center2 filter	772
config log azure-security-center2 setting	776
config log custom-field	778
config log disk filter	778
config log disk setting	782
config log eventfilter	788
config log fortianalyzer filter	791
config log fortianalyzer override-filter	795
config log fortianalyzer override-setting	799
config log fortianalyzer setting	804
config log fortianalyzer2 filter	808
config log fortianalyzer2 override-filter	812
config log fortianalyzer2 override-setting	816
config log fortianalyzer2 setting	821
config log fortianalyzer3 filter	826
config log fortianalyzer3 override-filter	830
config log fortianalyzer3 override-setting	834
config log fortianalyzer3 setting	839
config log fortianalyzer-cloud filter	843
config log fortianalyzer-cloud override-filter	847
config log fortianalyzer-cloud override-setting	851
config log fortianalyzer-cloud setting	852
config log fortiguard filter	856
config log fortiguard override-filter	860
config log fortiguard override-setting	863
config log fortiguard setting	865
config log gui-display	868
config log memory filter	869
config log memory global-setting	873
config log memory setting	874
config log null-device filter	874
config log null-device setting	878
config log setting	879
config log syslogd filter	884
config log syslogd override-filter	888
config log syslogd override-setting	892
config log syslogd setting	896
config log syslogd2 filter	900
config log syslogd2 override-filter	904
config log syslogd2 override-setting	908
config log syslogd2 setting	913
config log syslogd3 filter	917
config log syslogd3 override-filter	921
config log syslogd3 override-setting	925
config log syslogd3 setting	929

config log syslogd4 filter	933
config log syslogd4 override-filter	937
config log syslogd4 override-setting	941
config log syslogd4 setting	946
config log tacacs+accounting filter	950
config log tacacs+accounting setting	951
config log tacacs+accounting2 filter	952
config log tacacs+accounting2 setting	953
config log tacacs+accounting3 filter	954
config log tacacs+accounting3 setting	955
config log threat-weight	956
config log webtrends filter	967
config log webtrends setting	971
monitoring	972
config monitoring np6-ipsec-engine	972
config monitoring npu-hpe	973
nsxt	975
config nsxt service-chain	975
config nsxt setting	977
report	978
config report layout	978
config report setting	987
router	989
config router access-list	989
config router access-list6	991
config router aspath-list	992
config router auth-path	993
config router bfd	993
config router bfd6	995
config router bgp	996
config router community-list	1062
config router extcommunity-list	1063
config router isis	1064
config router key-chain	1078
config router multicast	1079
config router multicast6	1090
config router multicast-flow	1092
config router ospf	1093
config router ospf6	1110
config router policy	1124
config router policy6	1127
config router prefix-list	1130
config router prefix-list6	1131
config router rip	1132
config router ripng	1139
config router route-map	1145
config router setting	1151
config router static	1152
config router static6	1154

rule	1157
config rule fmwp	1157
config rule iotd	1159
config rule otdd	1161
config rule otvp	1163
sctp-filter	1166
config sctp-filter profile	1166
ssh-filter	1168
config ssh-filter profile	1168
switch-controller	1172
config switch-controller 802-1X-settings	1173
config switch-controller acl group	1176
config switch-controller acl ingress	1177
config switch-controller auto-config custom	1179
config switch-controller auto-config default	1181
config switch-controller auto-config policy	1182
config switch-controller custom-command	1184
config switch-controller dsl policy	1185
config switch-controller dynamic-port-policy	1188
config switch-controller flow-tracking	1192
config switch-controller fortilink-settings	1196
config switch-controller global	1198
config switch-controller igmp-snooping	1204
config switch-controller initial-config template	1206
config switch-controller initial-config vlans	1208
config switch-controller lldp-profile	1210
config switch-controller lldp-settings	1215
config switch-controller location	1216
config switch-controller mac-policy	1221
config switch-controller managed-switch	1223
config switch-controller network-monitor-settings	1266
config switch-controller ptp interface-policy	1267
config switch-controller ptp profile	1268
config switch-controller qos dot1p-map	1270
config switch-controller qos ip-dscp-map	1274
config switch-controller qos qos-policy	1277
config switch-controller qos queue-policy	1278
config switch-controller quarantine	1281
config switch-controller remote-log	1282
config switch-controller security-policy 802-1X	1285
config switch-controller security-policy local-access	1290
config switch-controller sflow	1292
config switch-controller snmp-community	1293
config switch-controller snmp-sysinfo	1296
config switch-controller snmp-trap-threshold	1297
config switch-controller snmp-user	1299
config switch-controller storm-control	1301
config switch-controller storm-control-policy	1303
config switch-controller stp-instance	1305

config switch-controller stp-settings	1306
config switch-controller switch-group	1308
config switch-controller switch-interface-tag	1309
config switch-controller switch-log	1310
config switch-controller switch-profile	1311
config switch-controller system	1313
config switch-controller traffic-policy	1316
config switch-controller traffic-sniffer	1318
config switch-controller virtual-port-pool	1320
config switch-controller vlan-policy	1321
system	1323
config system 3g-modem custom	1327
config system accprofile	1328
config system acme	1340
config system admin	1342
config system affinity-interrupt	1349
config system affinity-packet-redistribution	1350
config system alarm	1351
config system alias	1354
config system api-user	1354
config system arp-table	1356
config system automation-action	1357
config system automation-condition	1363
config system automation-destination	1365
config system automation-stitch	1365
config system automation-trigger	1367
config system autoupdate schedule	1372
config system autoupdate tunneling	1373
config system auto-install	1374
config system auto-scale	1375
config system auto-script	1376
config system bypass	1378
config system central-management	1379
config system cloud-service	1385
config system console	1386
config system csf	1387
config system custom-language	1393
config system ddns	1393
config system dedicated-mgmt	1396
config system device-upgrade	1397
config system dhcp server	1401
config system dhcp6 server	1412
config system digital-io	1418
config system dnp3-proxy	1419
config system dns	1421
config system dns64	1424
config system dns-database	1425
config system dns-server	1429
config system dscp-based-priority	1430

config system elbc	1432
config system email-server	1433
config system evpn	1435
config system external-resource	1436
config system fabric-vpn	1440
config system federated-upgrade	1444
config system fips-cc	1449
config system fortiguard	1450
config system fortindr	1460
config system fortisandbox	1461
config system fsso-polling	1463
config system ftm-push	1464
config system geneve	1465
config system geoip-override	1466
config system global	1468
config system gre-tunnel	1517
config system ha	1519
config system ha-monitor	1534
config system health-check-fortiguard	1535
config system icond	1536
config system ike	1541
config system interface	1554
config system ipam	1625
config system ipip-tunnel	1628
config system ips	1629
config system ipsec-aggregate	1630
config system ips-urlfilter-dns	1631
config system ips-urlfilter-dns6	1632
config system ipv6-neighbor-cache	1632
config system ipv6-tunnel	1633
config system iscsi	1634
config system isf-queue-profile	1636
config system link-monitor	1638
config system lldp network-policy	1643
config system lte-modem	1651
config system mac-address-table	1659
config system management-tunnel	1660
config system mobile-tunnel	1661
config system modem	1664
config system nd-proxy	1671
config system netflow	1672
config system network-visibility	1674
config system ngfw-settings	1675
config system np6	1676
config system np6xlite	1689
config system npu	1703
config system npu-post	1797
config system npu-setting prp	1798
config system npu-vlink	1799

config system ntp	1800
config system object-tagging	1803
config system password-policy	1805
config system password-policy-guest-admin	1807
config system pcp-server	1809
config system physical-switch	1812
config system pppoe-interface	1813
config system probe-response	1816
config system proxy-arp	1817
config system ptp	1818
config system replacemsg admin	1819
config system replacemsg alertmail	1820
config system replacemsg auth	1821
config system replacemsg automation	1822
config system replacemsg custom-message	1823
config system replacemsg fortiguard-wf	1824
config system replacemsg ftp	1826
config system replacemsg http	1827
config system replacemsg icap	1828
config system replacemsg mail	1829
config system replacemsg nac-quar	1830
config system replacemsg spam	1831
config system replacemsg sslvpn	1832
config system replacemsg traffic-quota	1833
config system replacemsg utm	1834
config system replacemsg webproxy	1836
config system replacemsg-group	1837
config system replacemsg-image	1850
config system resource-limits	1850
config system saml	1853
config system sdn-connector	1857
config system sdn-proxy	1866
config system sdn-vpn	1867
config system sdwan	1869
config system security-rating controls	1895
config system security-rating settings	1896
config system serial-port	1897
config system session-helper	1898
config system session-ttl	1899
config system settings	1900
config system sflow	1926
config system sit-tunnel	1927
config system smc-ntp	1929
config system sms-server	1930
config system snmp community	1931
config system snmp mib-view	1940
config system snmp rmon-stat	1941
config system snmp sysinfo	1942
config system snmp user	1944

config system speed-test-schedule	1951
config system speed-test-server	1954
config system speed-test-setting	1955
config system ssh-config	1956
config system sso-admin	1960
config system sso-forticloud-admin	1960
config system sso-fortigate-cloud-admin	1961
config system standalone-cluster	1961
config system storage	1966
config system stp	1968
config system switch-interface	1969
config system timezone	1971
config system tos-based-priority	1972
config system vdom	1973
config system vdom-dns	1973
config system vdom-exception	1975
config system vdom-link	1977
config system vdom-netflow	1978
config system vdom-property	1980
config system vdom-radius-server	1982
config system vdom-sflow	1982
config system vin-alarm	1984
config system virtual-switch	1986
config system virtual-wire-pair	1988
config system vene-interface	1989
config system vpce	1991
config system vxlan	1992
config system wccp	1993
config system wireless ap-status	1998
config system wireless settings	1999
config system zone	2002
telemetry-controller	2004
config telemetry-controller agent	2004
config telemetry-controller agent-profile	2006
config telemetry-controller application predefine	2007
config telemetry-controller global	2008
config telemetry-controller profile	2009
user	2013
config user adgrp	2013
config user certificate	2014
config user domain-controller	2015
config user exchange	2019
config user external-identity-provider	2021
config user fortitoken	2023
config user fsso	2024
config user fsso-polling	2028
config user group	2030
config user krb-keytab	2035
config user ldap	2036

config user local	2045
config user nac-policy	2048
config user password-policy	2051
config user peer	2053
config user peergrp	2055
config user pop3	2056
config user quarantine	2057
config user radius	2058
config user saml	2074
config user scim	2078
config user security-exempt-list	2080
config user setting	2081
config user tacacs+	2086
videofilter	2089
config videofilter keyword	2089
config videofilter profile	2090
config videofilter youtube-key	2093
virtual-patch	2094
config virtual-patch profile	2094
voip	2096
config voip profile	2096
vpn	2121
config vpn certificate ca	2121
config vpn certificate crt	2123
config vpn certificate hsm-local	2125
config vpn certificate local	2129
config vpn certificate ocsip-server	2134
config vpn certificate remote	2135
config vpn certificate setting	2136
config vpn ipsec concentrator	2142
config vpn ipsec fec	2142
config vpn ipsec manualkey	2144
config vpn ipsec manualkey-interface	2146
config vpn ipsec phase1	2148
config vpn ipsec phase1-interface	2179
config vpn ipsec phase2	2216
config vpn ipsec phase2-interface	2230
config vpn kmip-server	2244
config vpn l2tp	2246
config vpn pptp	2248
config vpn qkd	2248
config vpn ssl settings	2250
config vpn ssl web portal	2262
config vpn ssl web realm	2278
config vpn ssl web user-bookmark	2280
config vpn ssl web user-group-bookmark	2288
waf	2296
config waf main-class	2296
config waf profile	2296

config waf signature	2321
config waf sub-class	2321
wanopt	2322
config wanopt auth-group	2322
config wanopt cache-service	2324
config wanopt content-delivery-network-rule	2327
config wanopt peer	2333
config wanopt profile	2334
config wanopt remote-storage	2343
config wanopt settings	2344
config wanopt webcache	2346
web-proxy	2350
config web-proxy debug-url	2350
config web-proxy explicit	2351
config web-proxy fast-fallback	2358
config web-proxy forward-server	2359
config web-proxy forward-server-group	2362
config web-proxy global	2363
config web-proxy isolator-server	2368
config web-proxy profile	2369
config web-proxy url-match	2374
config web-proxy wisp	2375
webfilter	2377
config webfilter content	2377
config webfilter content-header	2379
config webfilter fortiguard	2380
config webfilter ftgd-local-cat	2382
config webfilter ftgd-local-rating	2383
config webfilter ftgd-local-risk	2384
config webfilter ftgd-risk-level	2385
config webfilter ips-urlfilter-cache-setting	2385
config webfilter ips-urlfilter-setting	2386
config webfilter ips-urlfilter-setting6	2387
config webfilter override	2387
config webfilter profile	2389
config webfilter search-engine	2406
config webfilter urlfilter	2408
wireless-controller	2412
config wireless-controller access-control-list	2413
config wireless-controller apcfg-profile	2415
config wireless-controller ap-status	2417
config wireless-controller arp-profile	2418
config wireless-controller ble-profile	2421
config wireless-controller bonjour-profile	2424
config wireless-controller global	2426
config wireless-controller hotspot20 anqp-3gpp-cellular	2431
config wireless-controller hotspot20 anqp-ip-address-type	2432
config wireless-controller hotspot20 anqp-nai-realm	2433
config wireless-controller hotspot20 anqp-network-auth-type	2437

config wireless-controller hotspot20 anqp-roaming-consortium	2438
config wireless-controller hotspot20 anqp-venue-name	2439
config wireless-controller hotspot20 anqp-venue-url	2439
config wireless-controller hotspot20 h2qp-advice-of-charge	2440
config wireless-controller hotspot20 h2qp-conn-capability	2442
config wireless-controller hotspot20 h2qp-operator-name	2445
config wireless-controller hotspot20 h2qp-osu-provider	2445
config wireless-controller hotspot20 h2qp-osu-provider-nai	2447
config wireless-controller hotspot20 h2qp-terms-and-conditions	2448
config wireless-controller hotspot20 h2qp-wan-metric	2449
config wireless-controller hotspot20 hs-profile	2450
config wireless-controller hotspot20 icon	2458
config wireless-controller hotspot20 qos-map	2459
config wireless-controller inter-controller	2461
config wireless-controller log	2463
config wireless-controller mpsk-profile	2468
config wireless-controller nac-profile	2471
config wireless-controller qos-profile	2472
config wireless-controller region	2475
config wireless-controller setting	2476
config wireless-controller snmp	2486
config wireless-controller ssid-policy	2490
config wireless-controller syslog-profile	2491
config wireless-controller timers	2493
config wireless-controller vap	2496
config wireless-controller vap-group	2528
config wireless-controller wag-profile	2529
config wireless-controller wids-profile	2530
config wireless-controller wtp	2548
config wireless-controller wtp-group	2571
config wireless-controller wtp-profile	2574
ztna	2662
config ztna reverse-connector	2662
config ztna traffic-forward-proxy	2663
config ztna web-portal	2664
config ztna web-portal-bookmark	2668
config ztna web-proxy	2675
CLI diagnose commands	2707
diagnose alertconsole	2711
diagnose alertconsole clear	2711
diagnose alertconsole fgd-retrieve	2711
diagnose alertconsole list	2711
diagnose alertconsole test	2712
diagnose antivirus	2712
diagnose antivirus database-info	2712
diagnose antivirus outbreak-prevention	2712
diagnose antivirus outbreak-prevention statistics	2712
diagnose antivirus outbreak-prevention statistics flush	2713
diagnose antivirus outbreak-prevention statistics list	2713

diagnose antivirus quarantine	2713
diagnose antivirus quarantine delete	2713
diagnose antivirus quarantine list	2713
diagnose antivirus quarantine purge	2714
diagnose antivirus test	2714
diagnose automation	2714
diagnose automation test	2714
diagnose autoupdate	2714
diagnose autoupdate downgrade	2715
diagnose autoupdate downgrade disable	2715
diagnose autoupdate downgrade enable	2715
diagnose autoupdate status	2715
diagnose autoupdate versions	2715
diagnose azure events	2715
diagnose azure events migration	2716
diagnose casb	2716
diagnose casb build	2716
diagnose casb show	2716
diagnose casb show app-attributes	2717
diagnose casb show app-details	2717
diagnose casb show app-domains	2717
diagnose casb show applications	2717
diagnose casb show apps	2717
diagnose casb show domains	2717
diagnose casb show isdb	2718
diagnose casb show isdb-all	2718
diagnose casb show isdb-name	2718
diagnose casb show isdb-uuid	2718
diagnose casb verify	2718
diagnose casb verify casb-isdb	2718
diagnose central-mgmt	2719
diagnose central-mgmt script-history	2719
diagnose central-mgmt script-history clear	2719
diagnose central-mgmt script-history del	2719
diagnose central-mgmt script-history list	2719
diagnose central-mgmt script-history test	2720
diagnose cid	2720
diagnose cid debug	2720
diagnose cid debug filter	2721
diagnose cid debug filter clear	2721
diagnose cid debug filter clear mac	2721
diagnose cid debug filter mac	2721
diagnose cid debug start	2721
diagnose cid debug stop	2721
diagnose cid restart	2722
diagnose cid scan	2722
diagnose cid scan csf	2722
diagnose cid scan ethernet	2722

diagnose cid scan lldp	2723
diagnose cid stats	2723
diagnose cid stats config	2723
diagnose cid stats crash	2723
diagnose cid stats debug	2723
diagnose cid stats manager	2724
diagnose cid stats scan	2724
diagnose cid stats trap	2724
diagnose cid stats unpack	2724
diagnose clearpass	2724
diagnose clearpass delete	2725
diagnose clearpass flush	2725
diagnose clearpass list	2725
diagnose clearpass list address	2725
diagnose clearpass list spt	2725
diagnose clearpass list summary	2726
diagnose debug	2726
diagnose debug admin	2733
diagnose debug admin error-log	2734
diagnose debug application	2734
diagnose debug application acd	2734
diagnose debug application acid	2734
diagnose debug application alarmd	2734
diagnose debug application alertmail	2735
diagnose debug application alicloud-ha	2735
diagnose debug application alicloud-sdn	2735
diagnose debug application authd	2735
diagnose debug application autod	2736
diagnose debug application awsd	2736
diagnose debug application azd	2736
diagnose debug application azd-ha	2736
diagnose debug application bfdd	2737
diagnose debug application cert-update	2737
diagnose debug application chassis	2737
diagnose debug application clearpass	2737
diagnose debug application cloudapid	2738
diagnose debug application cloudinitd	2738
diagnose debug application cmp	2738
diagnose debug application crl-update	2738
diagnose debug application csfd	2738
diagnose debug application cu_acd	2739
diagnose debug application cw_acd	2739
diagnose debug application cw_acd_helper	2739
diagnose debug application cw_acd_wlev	2740
diagnose debug application cw_acd_wpad	2740
diagnose debug application ddnsd	2740
diagnose debug application dhcp6c	2740
diagnose debug application dhcp6r	2741
diagnose debug application dhcp6s	2741

diagnose debug application dhcpd	2741
diagnose debug application dhcprelay	2741
diagnose debug application dhcps	2741
diagnose debug application dlpfingerprint	2742
diagnose debug application dnp	2742
diagnose debug application dnsproxy	2742
diagnose debug application eap_proxy	2742
diagnose debug application eap_supp	2743
diagnose debug application est	2743
diagnose debug application evpnd	2743
diagnose debug application extenderd	2743
diagnose debug application fclfd	2744
diagnose debug application fcnacd	2744
diagnose debug application fds_notify	2744
diagnose debug application fgd_alert	2744
diagnose debug application fgfmd	2744
diagnose debug application fgtlogd	2745
diagnose debug application flcfd	2745
diagnose debug application flpold	2745
diagnose debug application fltund	2745
diagnose debug application fnbamd	2746
diagnose debug application foauthd	2746
diagnose debug application forticldd	2746
diagnose debug application forticron	2746
diagnose debug application fortlinkd	2747
diagnose debug application fortimq	2747
diagnose debug application fsso_ldap	2747
diagnose debug application fssod	2747
diagnose debug application fsvrd	2747
diagnose debug application ftm-push	2748
diagnose debug application garpd	2748
diagnose debug application gcpd	2748
diagnose debug application hamonitor	2748
diagnose debug application harelay	2749
diagnose debug application hasync	2749
diagnose debug application hataik	2749
diagnose debug application httpsd	2749
diagnose debug application ibmd	2750
diagnose debug application icond	2750
diagnose debug application ike	2750
diagnose debug application ikecrypt	2750
diagnose debug application imap	2751
diagnose debug application init	2751
diagnose debug application iotd	2751
diagnose debug application ipamd	2751
diagnose debug application ipamsd	2752
diagnose debug application ipdbd	2752
diagnose debug application ipsengine	2752
diagnose debug application ipsmonitor	2752

diagnose debug application ipsufd	2752
diagnose debug application kmiglogd	2753
diagnose debug application kmipd	2753
diagnose debug application kubed	2753
diagnose debug application l2tp	2753
diagnose debug application link-monitor	2754
diagnose debug application link-monitor-passive	2754
diagnose debug application locallogd	2754
diagnose debug application lpmd	2754
diagnose debug application miglogd	2755
diagnose debug application mrd	2755
diagnose debug application netxd	2755
diagnose debug application nntp	2755
diagnose debug application nodejs	2755
diagnose debug application npd	2756
diagnose debug application ntnxd	2756
diagnose debug application ntpd	2756
diagnose debug application oaas_agent	2756
diagnose debug application ocid	2757
diagnose debug application openstackd	2757
diagnose debug application ovrd	2757
diagnose debug application pcpd	2757
diagnose debug application pop3	2758
diagnose debug application ppp	2758
diagnose debug application pppoed	2758
diagnose debug application pptp	2758
diagnose debug application pptpc	2758
diagnose debug application proxy	2759
diagnose debug application ptpd	2759
diagnose debug application quarantine	2759
diagnose debug application radius-das	2759
diagnose debug application radiusd	2760
diagnose debug application radvd	2760
diagnose debug application reportd	2760
diagnose debug application route-tag	2760
diagnose debug application samld	2761
diagnose debug application sapd	2761
diagnose debug application sccp	2761
diagnose debug application scep	2761
diagnose debug application scimd	2762
diagnose debug application sdncd	2762
diagnose debug application sdnvpnd	2762
diagnose debug application sdwan	2762
diagnose debug application sepmd	2762
diagnose debug application server-probe	2763
diagnose debug application sessionsync	2763
diagnose debug application sflowd	2763
diagnose debug application sfupgraded	2763
diagnose debug application sip	2764

diagnose debug application smbcd	2764
diagnose debug application smtp	2764
diagnose debug application snmpd	2764
diagnose debug application spareblock	2765
diagnose debug application speedtest	2765
diagnose debug application speedtestd	2765
diagnose debug application sshd	2765
diagnose debug application sslvpn	2765
diagnose debug application syslogd	2766
diagnose debug application update	2766
diagnose debug application uploadd	2766
diagnose debug application urlfilter	2766
diagnose debug application vmwd	2767
diagnose debug application vned	2767
diagnose debug application vrrpd	2767
diagnose debug application wabcs	2767
diagnose debug application waocs	2768
diagnose debug application wccpd	2768
diagnose debug application wf_monitor	2768
diagnose debug application wifi	2768
diagnose debug application wpa-show-keys	2768
diagnose debug application wpa-timestamp	2769
diagnose debug application wpad	2769
diagnose debug application wpad-crash-hexdump	2769
diagnose debug application zebos	2769
diagnose debug application zebos-launcher	2770
diagnose debug authd	2770
diagnose debug authd clear	2770
diagnose debug authd fsso	2770
diagnose debug authd fsso add-address	2770
diagnose debug authd fsso clear-logons	2771
diagnose debug authd fsso del-address	2771
diagnose debug authd fsso filter	2771
diagnose debug authd fsso filter clear	2771
diagnose debug authd fsso filter group	2772
diagnose debug authd fsso filter server	2772
diagnose debug authd fsso filter source	2772
diagnose debug authd fsso filter user	2772
diagnose debug authd fsso flush-address	2773
diagnose debug authd fsso flush-address-all	2773
diagnose debug authd fsso list	2773
diagnose debug authd fsso refresh-groups	2773
diagnose debug authd fsso refresh-logons	2773
diagnose debug authd fsso server-status	2773
diagnose debug authd fsso show-address	2774
diagnose debug authd fsso summary	2774
diagnose debug authd memory	2774
diagnose debug aws-vpce	2774
diagnose debug backtrace	2774

diagnose debug cli	2774
diagnose debug cloudinit	2775
diagnose debug cloudinit clear	2775
diagnose debug cloudinit show	2775
diagnose debug cmdb-trace	2775
diagnose debug cmdb-walk	2775
diagnose debug config-error-log	2776
diagnose debug config-error-log clear	2776
diagnose debug config-error-log read	2776
diagnose debug console	2776
diagnose debug console no-user-log-msg	2776
diagnose debug console no-user-log-msg disable	2776
diagnose debug console no-user-log-msg enable	2777
diagnose debug console retry-log-msg	2777
diagnose debug console retry-log-msg disable	2777
diagnose debug console retry-log-msg enable	2777
diagnose debug console send	2777
diagnose debug console timestamp	2778
diagnose debug console timestamp disable	2778
diagnose debug console timestamp enable	2778
diagnose debug crashlog	2778
diagnose debug crashlog clear	2778
diagnose debug crashlog get	2778
diagnose debug crashlog history	2779
diagnose debug crashlog interval	2779
diagnose debug disable	2779
diagnose debug duration	2779
diagnose debug enable	2779
diagnose debug flow	2780
diagnose debug flow filter	2780
diagnose debug flow filter addr	2780
diagnose debug flow filter clear	2780
diagnose debug flow filter daddr	2780
diagnose debug flow filter dport	2781
diagnose debug flow filter negate	2781
diagnose debug flow filter negate addr	2781
diagnose debug flow filter negate daddr	2781
diagnose debug flow filter negate dport	2781
diagnose debug flow filter negate port	2781
diagnose debug flow filter negate proto	2782
diagnose debug flow filter negate saddr	2782
diagnose debug flow filter negate sport	2782
diagnose debug flow filter negate vd	2782
diagnose debug flow filter port	2782
diagnose debug flow filter proto	2782
diagnose debug flow filter saddr	2783
diagnose debug flow filter sport	2783
diagnose debug flow filter vd	2783
diagnose debug flow filter vd-name	2783

diagnose debug flow filter6	2784
diagnose debug flow filter6 addr	2784
diagnose debug flow filter6 clear	2784
diagnose debug flow filter6 daddr	2784
diagnose debug flow filter6 dport	2785
diagnose debug flow filter6 negate	2785
diagnose debug flow filter6 negate addr	2785
diagnose debug flow filter6 negate daddr	2785
diagnose debug flow filter6 negate dport	2785
diagnose debug flow filter6 negate port	2785
diagnose debug flow filter6 negate proto	2786
diagnose debug flow filter6 negate saddr	2786
diagnose debug flow filter6 negate sport	2786
diagnose debug flow filter6 negate vd	2786
diagnose debug flow filter6 port	2786
diagnose debug flow filter6 proto	2786
diagnose debug flow filter6 saddr	2787
diagnose debug flow filter6 sport	2787
diagnose debug flow filter6 vd	2787
diagnose debug flow filter6 vd-name	2787
diagnose debug flow show	2788
diagnose debug flow show function-name	2788
diagnose debug flow show function-name disable	2788
diagnose debug flow show function-name enable	2788
diagnose debug flow show iprope	2788
diagnose debug flow show iprope disable	2788
diagnose debug flow show iprope enable	2789
diagnose debug flow trace	2789
diagnose debug flow trace start	2789
diagnose debug flow trace start6	2789
diagnose debug flow trace stop	2789
diagnose debug flow trace stop6	2790
diagnose debug fortalink-report	2790
diagnose debug fortalink-report all	2790
diagnose debug fortalink-report switch-group	2790
diagnose debug fortalink-report switch-id	2790
diagnose debug fortism	2791
diagnose debug fortism enable	2791
diagnose debug fsso-polling	2791
diagnose debug fsso-polling client	2791
diagnose debug fsso-polling detail	2791
diagnose debug fsso-polling group	2791
diagnose debug fsso-polling refresh-user	2792
diagnose debug fsso-polling set-log-source	2792
diagnose debug fsso-polling summary	2792
diagnose debug fsso-polling user	2792
diagnose debug info	2793
diagnose debug kernel	2793
diagnose debug kernel ha	2793

diagnose debug kernel level	2793
diagnose debug kernel sysrq	2793
diagnose debug kernel sysrq command	2794
diagnose debug kernel sysrq command crash	2794
diagnose debug kernel sysrq disable	2794
diagnose debug kernel sysrq enable	2794
diagnose debug kernel sysrq status	2794
diagnose debug rating	2794
diagnose debug report	2795
diagnose debug report reset	2795
diagnose debug reset	2795
diagnose debug sdnc	2795
diagnose debug sdnc valgrind	2795
diagnose debug sdnc valgrind disable	2795
diagnose debug sdnc valgrind enable	2796
diagnose debug sdnc valgrind log	2796
diagnose debug sdnc valgrind log clear	2796
diagnose debug sdnc valgrind log show	2796
diagnose debug sdnc valgrind memcheck	2796
diagnose debug sdnc valgrind memcheck_less	2796
diagnose debug sdnc valgrind status	2797
diagnose debug sql-log-error	2797
diagnose debug sql-log-error clear	2797
diagnose debug sql-log-error read	2797
diagnose debug sql-log-error status	2797
diagnose debug traffic	2797
diagnose debug traffic dump-debug	2798
diagnose debug traffic error	2798
diagnose debug traffic history	2798
diagnose debug traffic interface	2798
diagnose debug traffic peek	2798
diagnose debug urlfilter	2799
diagnose debug urlfilter src-addr	2799
diagnose debug urlfilter test-url	2799
diagnose debug urlfilter valgrind	2799
diagnose debug urlfilter valgrind disable	2799
diagnose debug urlfilter valgrind enable	2800
diagnose debug urlfilter valgrind log	2800
diagnose debug urlfilter valgrind log clear	2800
diagnose debug urlfilter valgrind log show	2800
diagnose debug urlfilter valgrind memcheck	2800
diagnose debug urlfilter valgrind memcheck_less	2800
diagnose debug urlfilter valgrind status	2801
diagnose debug user	2801
diagnose debug user hash	2801
diagnose debug user list	2801
diagnose debug vm-print-license	2801
diagnose debug vpce	2801
diagnose disktest	2802

diagnose disktest block	2802
diagnose disktest block 1	2802
diagnose disktest block 16	2802
diagnose disktest block 256	2802
diagnose disktest block 4	2803
diagnose disktest block 64	2803
diagnose disktest device	2803
diagnose disktest run	2803
diagnose disktest size	2803
diagnose disktest time	2804
diagnose dpdk config	2804
diagnose dpdk config show	2804
diagnose dpdk log clear	2804
diagnose dpdk log clear early-init	2804
diagnose dpdk log show	2805
diagnose dpdk log show early-init	2805
diagnose dpdk performance	2805
diagnose dpdk performance show	2805
diagnose dpdk statistics clear	2805
diagnose dpdk statistics clear all	2805
diagnose dpdk statistics show	2806
diagnose dpdk statistics show engine	2806
diagnose dpdk statistics show ipsec	2806
diagnose dpdk statistics show memory	2806
diagnose dpdk statistics show port	2806
diagnose dpdk statistics show vnp	2807
diagnose dpdk version	2807
diagnose dpdk version show	2807
diagnose emailfilter	2807
diagnose emailfilter bword	2807
diagnose emailfilter bword matchfilter	2808
diagnose emailfilter fortishield	2808
diagnose emailfilter fortishield servers	2808
diagnose emailfilter fortishield statistics	2808
diagnose emailfilter fortishield statistics flush	2808
diagnose emailfilter fortishield statistics list	2809
diagnose endpoint	2809
diagnose endpoint avatar	2811
diagnose endpoint avatar allow-nodisk	2811
diagnose endpoint avatar cleanup	2811
diagnose endpoint avatar find	2811
diagnose endpoint avatar find fingerprint	2812
diagnose endpoint avatar find uid	2812
diagnose endpoint avatar list	2812
diagnose endpoint avatar list active	2812
diagnose endpoint avatar list all	2812
diagnose endpoint avatar list inactive	2813
diagnose endpoint avatar purge-all	2813

diagnose endpoint debug-zone	2813
diagnose endpoint debug-zone background-debug	2813
diagnose endpoint debug-zone dump	2813
diagnose endpoint debug-zone set-lls-quota	2814
diagnose endpoint ec-shm	2814
diagnose endpoint ec-shm delete	2814
diagnose endpoint ec-shm find-by-ipvd	2814
diagnose endpoint ec-shm find-by-uid	2815
diagnose endpoint ec-shm list	2815
diagnose endpoint ec-shm summary	2815
diagnose endpoint ec-shm update-by-json	2815
diagnose endpoint fctems	2816
diagnose endpoint fctems api-status	2816
diagnose endpoint fctems api-status clear	2816
diagnose endpoint fctems cloud-server	2816
diagnose endpoint fctems custom	2817
diagnose endpoint fctems ec-shm-dump	2817
diagnose endpoint fctems get-pub-addr	2817
diagnose endpoint fctems info	2817
diagnose endpoint fctems info pause	2818
diagnose endpoint fctems info pre-master-key	2818
diagnose endpoint fctems info protocol	2818
diagnose endpoint fctems info repeat	2818
diagnose endpoint fctems info repeat data-in	2818
diagnose endpoint fctems info repeat data-out	2819
diagnose endpoint fctems info repeat header-in	2819
diagnose endpoint fctems info repeat header-out	2819
diagnose endpoint fctems info repeat ssl-data-in	2819
diagnose endpoint fctems info repeat ssl-data-out	2819
diagnose endpoint fctems info repeat textinfo	2820
diagnose endpoint fctems info reset	2820
diagnose endpoint fctems info resume	2820
diagnose endpoint fctems json	2820
diagnose endpoint fctems json deep-inspect-cert-sync	2820
diagnose endpoint fctems json gateway-mac-request	2821
diagnose endpoint fctems queue-complete-calls	2821
diagnose endpoint fctems test-authorization	2821
diagnose endpoint fctems test-connectivity	2821
diagnose endpoint fctems wss-cert-skip-check	2821
diagnose endpoint filter	2822
diagnose endpoint filter avatar-fingerprint	2822
diagnose endpoint filter clear	2822
diagnose endpoint filter ems-sn	2822
diagnose endpoint filter ftcl-uid	2822
diagnose endpoint filter list	2823
diagnose endpoint filter record-debug-log	2823
diagnose endpoint filter show-large-data	2823
diagnose endpoint lls-comm	2823
diagnose endpoint lls-comm connect	2823

diagnose endpoint lls-comm disconnect	2824
diagnose endpoint lls-comm recv	2824
diagnose endpoint lls-comm send	2824
diagnose endpoint lls-comm send echo	2824
diagnose endpoint lls-comm send echo echo	2824
diagnose endpoint lls-comm send general	2825
diagnose endpoint lls-comm send general get-index	2825
diagnose endpoint lls-comm send general register	2825
diagnose endpoint lls-comm send general unregister	2825
diagnose endpoint lls-comm send ping	2825
diagnose endpoint lls-comm send ping set-interval	2826
diagnose endpoint lls-comm send ztna	2826
diagnose endpoint lls-comm send ztna find-ip-vdom	2826
diagnose endpoint lls-comm send ztna find-uid	2826
diagnose endpoint lls-comm send ztna message-format	2827
diagnose endpoint lls-comm send ztna subscribe-all	2827
diagnose endpoint lls-comm send ztna unsubscribe-all	2827
diagnose endpoint lls-comm send ztna unsubscribe-uid	2827
diagnose endpoint lls-comm status	2828
diagnose endpoint tags	2828
diagnose endpoint tags remove-by-id	2828
diagnose endpoint tags remove-by-name	2828
diagnose endpoint tags remove-by-name-legacy	2828
diagnose endpoint tags remove-by-sn	2829
diagnose endpoint tags test-common-tag-update	2829
diagnose extender	2829
diagnose extender atcmd	2829
diagnose extender cmd	2830
diagnose extender modem-list	2830
diagnose fdsm	2830
diagnose fdsm account-info	2831
diagnose fdsm central-mgmt-status	2831
diagnose fdsm cfg-diff	2831
diagnose fdsm cfg-download	2832
diagnose fdsm cfg-list	2832
diagnose fdsm cfg-upload	2832
diagnose fdsm contract-controller-update	2832
diagnose fdsm fap-fsw-fext-contract-download	2833
diagnose fdsm fc-installer-download	2833
diagnose fdsm fds-update	2833
diagnose fdsm fmg-auto-discovery-status	2833
diagnose fdsm fortiap-download	2833
diagnose fdsm fortiap-latest-ver	2834
diagnose fdsm forticlient-net-info	2834
diagnose fdsm forticlient-update	2834
diagnose fdsm fortiex-download	2834
diagnose fdsm fortiex-latest-ver	2834
diagnose fdsm fortisw-download	2835
diagnose fdsm fortisw-latest-ver	2835

diagnose fdsm ftk-activate	2835
diagnose fdsm image-download	2835
diagnose fdsm image-list	2836
diagnose fdsm image-upgrade-matrix	2836
diagnose fdsm log-controller-update	2836
diagnose fdsm message-update	2836
diagnose fdsm modem-list	2836
diagnose fdsm report-download	2836
diagnose fdsm report-list	2837
diagnose fdsm sslvpn-man-upgrade-package-download	2837
diagnose fdsm sslvpn-package-download	2837
diagnose ffdb-fqdn	2837
diagnose ffdb-fqdn custom-get	2838
diagnose ffdb-fqdn custom-list	2838
diagnose firewall	2838
diagnose firewall auth	2845
diagnose firewall auth clear	2845
diagnose firewall auth filter	2845
diagnose firewall auth filter clear	2845
diagnose firewall auth filter group	2845
diagnose firewall auth filter mac	2845
diagnose firewall auth filter method	2846
diagnose firewall auth filter policy	2846
diagnose firewall auth filter source	2846
diagnose firewall auth filter source6	2847
diagnose firewall auth filter user	2847
diagnose firewall auth ipv6	2847
diagnose firewall auth ipv6 clear	2847
diagnose firewall auth ipv6 list	2848
diagnose firewall auth list	2848
diagnose firewall auth mac	2848
diagnose firewall auth mac clear	2848
diagnose firewall auth mac list	2848
diagnose firewall blocking	2848
diagnose firewall blocking list	2849
diagnose firewall dns-xlate	2849
diagnose firewall dns-xlate mapping	2849
diagnose firewall dns-xlate mapping list	2849
diagnose firewall dns-xlate pool	2849
diagnose firewall dns-xlate pool list	2849
diagnose firewall dynamic	2850
diagnose firewall dynamic address	2850
diagnose firewall dynamic list	2850
diagnose firewall dynamic test-common-tag-update	2850
diagnose firewall dynamic6	2850
diagnose firewall dynamic6 address	2851
diagnose firewall dynamic6 list	2851
diagnose firewall fqdn	2851
diagnose firewall fqdn get-ip	2851

diagnose firewall fqdn get-mac	2851
diagnose firewall fqdn getinfo-ip	2852
diagnose firewall fqdn getinfo-mac	2852
diagnose firewall fqdn list-all	2852
diagnose firewall fqdn list-ip	2852
diagnose firewall fqdn list-mac	2852
diagnose firewall fqdn6	2853
diagnose firewall fqdn6 list	2853
diagnose firewall internet-service	2853
diagnose firewall internet-service list	2853
diagnose firewall internet-service-app-ctrl	2853
diagnose firewall internet-service-app-ctrl list	2853
diagnose firewall internet-service-app-ctrl6	2854
diagnose firewall internet-service-app-ctrl6 list	2854
diagnose firewall internet-service-cache	2854
diagnose firewall internet-service-cache list	2854
diagnose firewall internet-service-custom	2854
diagnose firewall internet-service-custom list	2855
diagnose firewall internet-service-disable	2855
diagnose firewall internet-service-disable list	2855
diagnose firewall internet-service-extension	2855
diagnose firewall internet-service-extension list	2855
diagnose firewall internet-service-prio-id	2856
diagnose firewall internet-service-prio-id list	2856
diagnose firewall internet-service6	2856
diagnose firewall internet-service6 list	2856
diagnose firewall internet-service6-cache	2856
diagnose firewall internet-service6-cache list	2856
diagnose firewall internet-service6-custom	2857
diagnose firewall internet-service6-custom list	2857
diagnose firewall internet-service6-disable	2857
diagnose firewall internet-service6-disable list	2857
diagnose firewall internet-service6-extension	2857
diagnose firewall internet-service6-extension list	2858
diagnose firewall internet-service6-prio-id	2858
diagnose firewall internet-service6-prio-id list	2858
diagnose firewall ip-translation	2858
diagnose firewall ip-translation list	2858
diagnose firewall ipgeo	2858
diagnose firewall ipgeo copyright-notice	2859
diagnose firewall ipgeo country-list	2859
diagnose firewall ipgeo ip-list	2859
diagnose firewall ipgeo ip2country	2859
diagnose firewall ipgeo ip6-list	2859
diagnose firewall ipgeo override	2860
diagnose firewall iplist	2860
diagnose firewall iplist list	2860
diagnose firewall iplist list optimized	2860
diagnose firewall iplist6	2860

diagnose firewall iplist6 list	2860
diagnose firewall iplist6 list optimized	2861
diagnose firewall ipmac	2861
diagnose firewall ipmac add	2861
diagnose firewall ipmac delete	2861
diagnose firewall ipmac list	2861
diagnose firewall ipmac status	2862
diagnose firewall ippool	2862
diagnose firewall ippool filter	2862
diagnose firewall ippool filter clear	2862
diagnose firewall ippool filter name	2862
diagnose firewall ippool list	2862
diagnose firewall ippool list nat-ip	2863
diagnose firewall ippool list pba	2863
diagnose firewall ippool list user	2863
diagnose firewall ippool reset-log-stats	2863
diagnose firewall ippool stats	2863
diagnose firewall ippool-all	2863
diagnose firewall ippool-all list	2864
diagnose firewall ippool-all stats	2864
diagnose firewall ippool-fixed-range	2864
diagnose firewall ippool-fixed-range list	2864
diagnose firewall ippool-fixed-range list natip	2864
diagnose firewall ippool-nptv6	2865
diagnose firewall ippool-nptv6 natip	2865
diagnose firewall iprope	2865
diagnose firewall iprope appctrl	2865
diagnose firewall iprope appctrl list	2865
diagnose firewall iprope appctrl shaper	2865
diagnose firewall iprope appctrl shaper list	2866
diagnose firewall iprope appctrl stats	2866
diagnose firewall iprope appctrl stats clear	2866
diagnose firewall iprope appctrl stats list	2866
diagnose firewall iprope appctrl status	2866
diagnose firewall iprope clear	2866
diagnose firewall iprope list	2867
diagnose firewall iprope lookup	2867
diagnose firewall iprope show	2867
diagnose firewall iprope state	2868
diagnose firewall iprope top	2868
diagnose firewall iprope6	2868
diagnose firewall iprope6 clear	2868
diagnose firewall iprope6 list	2868
diagnose firewall iprope6 lookup	2869
diagnose firewall iprope6 show	2869
diagnose firewall iprope6 state	2869
diagnose firewall iprope6 top	2870
diagnose firewall ipv6-ehf	2870
diagnose firewall ipv6-ehf list	2870

diagnose firewall network-service-dynamic	2870
diagnose firewall network-service-dynamic list	2870
diagnose firewall ngfw-fix-application	2871
diagnose firewall ngfw-fix-application list	2871
diagnose firewall packet	2871
diagnose firewall packet distribution	2871
diagnose firewall pcp-mapping	2871
diagnose firewall pcp-mapping filter	2871
diagnose firewall pcp-mapping filter clear	2872
diagnose firewall pcp-mapping filter client-ip	2872
diagnose firewall pcp-mapping filter ext-ip	2872
diagnose firewall pcp-mapping filter ext-port	2872
diagnose firewall pcp-mapping filter intl-ip	2873
diagnose firewall pcp-mapping filter intl-port	2873
diagnose firewall pcp-mapping filter pool	2873
diagnose firewall pcp-mapping filter protocol	2873
diagnose firewall pcp-mapping filter remote-ip	2874
diagnose firewall pcp-mapping filter remote-port	2874
diagnose firewall pcp-mapping flush	2874
diagnose firewall pcp-mapping flush inbound	2874
diagnose firewall pcp-mapping flush outbound	2874
diagnose firewall pcp-mapping list	2875
diagnose firewall pcp-mapping list inbound	2875
diagnose firewall pcp-mapping list outbound	2875
diagnose firewall proute	2875
diagnose firewall proute clear	2875
diagnose firewall proute list	2875
diagnose firewall proute show	2876
diagnose firewall proute6	2876
diagnose firewall proute6 clear	2876
diagnose firewall proute6 list	2876
diagnose firewall proute6 show	2876
diagnose firewall route_tag	2877
diagnose firewall route_tag list	2877
diagnose firewall route_tag_v6	2877
diagnose firewall route_tag_v6 list	2877
diagnose firewall schedule	2877
diagnose firewall schedule debug	2878
diagnose firewall schedule list	2878
diagnose firewall schedule reload	2878
diagnose firewall sf-addresses	2878
diagnose firewall sf-addresses list	2878
diagnose firewall shaper	2878
diagnose firewall shaper dynamic-shaper	2879
diagnose firewall shaper dynamic-shaper flush	2879
diagnose firewall shaper dynamic-shaper list	2879
diagnose firewall shaper dynamic-shaper list ip	2879
diagnose firewall shaper dynamic-shaper list ipv6	2879
diagnose firewall shaper dynamic-shaper list user	2880

diagnose firewall shaper dynamic-shaper stats	2880
diagnose firewall shaper per-ip-shaper	2880
diagnose firewall shaper per-ip-shaper clear	2880
diagnose firewall shaper per-ip-shaper list	2880
diagnose firewall shaper per-ip-shaper state	2880
diagnose firewall shaper per-ip-shaper stats	2881
diagnose firewall shaper traffic-shaper	2881
diagnose firewall shaper traffic-shaper list	2881
diagnose firewall shaper traffic-shaper state	2881
diagnose firewall shaper traffic-shaper stats	2881
diagnose firewall shaper traffic-shaper stats clear	2881
diagnose firewall shaper traffic-shaper stats list	2882
diagnose firewall uuid	2882
diagnose firewall uuid list	2882
diagnose firewall vendor-mac	2882
diagnose firewall vendor-mac list	2882
diagnose firewall vip	2882
diagnose firewall vip realserver	2883
diagnose firewall vip realserver clear	2883
diagnose firewall vip realserver clear vip	2883
diagnose firewall vip realserver clear vip6	2883
diagnose firewall vip realserver down	2883
diagnose firewall vip realserver healthcheck	2884
diagnose firewall vip realserver healthcheck stats	2884
diagnose firewall vip realserver healthcheck stats clear	2884
diagnose firewall vip realserver healthcheck stats show	2884
diagnose firewall vip realserver list	2884
diagnose firewall vip realserver up	2885
diagnose firewall vip virtual-server	2885
diagnose firewall vip virtual-server filter	2885
diagnose firewall vip virtual-server filter clear	2885
diagnose firewall vip virtual-server filter dst	2885
diagnose firewall vip virtual-server filter dst-port	2886
diagnose firewall vip virtual-server filter list	2886
diagnose firewall vip virtual-server filter name	2886
diagnose firewall vip virtual-server filter negate	2886
diagnose firewall vip virtual-server filter negate dst-addr	2886
diagnose firewall vip virtual-server filter negate dst-port	2887
diagnose firewall vip virtual-server filter negate name	2887
diagnose firewall vip virtual-server filter negate src-addr	2887
diagnose firewall vip virtual-server filter negate src-port	2887
diagnose firewall vip virtual-server filter negate vd	2887
diagnose firewall vip virtual-server filter negate worker	2887
diagnose firewall vip virtual-server filter src	2888
diagnose firewall vip virtual-server filter src-port	2888
diagnose firewall vip virtual-server filter vd	2888
diagnose firewall vip virtual-server filter worker	2888
diagnose firewall vip virtual-server real-server	2889
diagnose firewall vip virtual-server real-server list	2889

diagnose firewall vip virtual-server stats	2889
diagnose firewall vip virtual-server stats clear	2889
diagnose firewall vip virtual-server stats crypto-clear	2889
diagnose firewall vip virtual-server stats http	2889
diagnose firewall vip virtual-server stats http all	2890
diagnose firewall vip virtual-server stats http clear	2890
diagnose firewall vip virtual-server stats http list	2890
diagnose firewall vip virtual-server stats list	2890
diagnose firewall vip virtual-server stats operational	2890
diagnose firewall vip virtual-server stats operational all	2890
diagnose firewall vip virtual-server stats operational list	2891
diagnose firewall vip virtual-server stats ssl	2891
diagnose firewall vip virtual-server stats ssl all	2891
diagnose firewall vip virtual-server stats ssl clear	2891
diagnose firewall vip virtual-server stats ssl list	2891
diagnose firewall vip virtual-server stats summary	2891
diagnose firewall vip virtual-server stats summary all	2892
diagnose firewall vip virtual-server stats summary clear	2892
diagnose firewall vip virtual-server stats summary list	2892
diagnose firewall vip virtual-server test	2892
diagnose firewall vip virtual-server test benchmark	2892
diagnose firewall vip virtual-server test benchmark dh-make-key	2892
diagnose firewall vip virtual-server test benchmark dh-make-secret	2893
diagnose firewall vip virtual-server test benchmark rand	2893
diagnose firewall vip virtual-server test benchmark rsa	2893
diagnose firewall vip virtual-server test benchmark rsa-mskb	2893
diagnose firewall vip virtual-server test key-exchange	2893
diagnose firewall vip virtual-server test key-exchange async	2893
diagnose firewall vip virtual-server test key-exchange sync	2894
diagnose firewall vip virtual-server test next-proto	2894
diagnose firewall vip virtual-server test next-proto disable	2894
diagnose firewall vip virtual-server test next-proto enable	2894
diagnose firewall vip virtual-server test rsa-blinding	2894
diagnose firewall vip virtual-server test rsa-blinding disable	2894
diagnose firewall vip virtual-server test rsa-blinding enable	2895
diagnose firewall vip virtual-server test ssl	2895
diagnose firewall vip virtual-server test ssl async	2895
diagnose firewall vip virtual-server test ssl sync	2895
diagnose forticare	2895
diagnose forticare cnreg-code-list	2896
diagnose forticare direct-registration	2896
diagnose forticare direct-registration country-data	2896
diagnose forticare direct-registration organization-list	2896
diagnose forticare direct-registration product-deregister	2896
diagnose forticare direct-registration product-registration	2897
diagnose forticare direct-registration product-transfer	2897
diagnose forticare direct-registration reseller-list	2897
diagnose fortiguard-resources	2897
diagnose fortiguard-resources delete	2899

diagnose fortiguard-resources delete app-categories	2899
diagnose fortiguard-resources delete app-info	2899
diagnose fortiguard-resources delete dlp-object	2900
diagnose fortiguard-resources delete fortiap-end-of-support	2900
diagnose fortiguard-resources delete fortixtender-end-of-support	2900
diagnose fortiguard-resources delete fortigate-end-of-support	2900
diagnose fortiguard-resources delete fortiswitch-end-of-support	2901
diagnose fortiguard-resources delete ips-information	2901
diagnose fortiguard-resources delete prefix-links	2901
diagnose fortiguard-resources delete sprite-casb	2901
diagnose fortiguard-resources delete sprite-isdb	2901
diagnose fortiguard-resources delete sprite-map	2901
diagnose fortiguard-resources delete static-links	2902
diagnose fortiguard-resources delete wf-categories	2902
diagnose fortiguard-resources delete-all	2902
diagnose fortiguard-resources downloads	2902
diagnose fortiguard-resources downloads disable	2902
diagnose fortiguard-resources downloads enable	2902
diagnose fortiguard-resources info	2903
diagnose fortiguard-resources info app-categories	2903
diagnose fortiguard-resources info app-info	2903
diagnose fortiguard-resources info dlp-object	2903
diagnose fortiguard-resources info fortiap-end-of-support	2903
diagnose fortiguard-resources info fortixtender-end-of-support	2904
diagnose fortiguard-resources info fortigate-end-of-support	2904
diagnose fortiguard-resources info fortiswitch-end-of-support	2904
diagnose fortiguard-resources info ips-information	2904
diagnose fortiguard-resources info prefix-links	2904
diagnose fortiguard-resources info sprite-casb.css	2905
diagnose fortiguard-resources info sprite-casb.png	2905
diagnose fortiguard-resources info sprite-isdb.css	2905
diagnose fortiguard-resources info sprite-isdb.png	2905
diagnose fortiguard-resources info sprite-map.css	2905
diagnose fortiguard-resources info sprite-map.png	2905
diagnose fortiguard-resources info static-links	2906
diagnose fortiguard-resources info wf-categories	2906
diagnose fortiguard-resources log	2906
diagnose fortiguard-resources log all	2906
diagnose fortiguard-resources log app-categories	2906
diagnose fortiguard-resources log app-info	2906
diagnose fortiguard-resources log fortiap-end-of-support	2907
diagnose fortiguard-resources log fortixtender-end-of-support	2907
diagnose fortiguard-resources log fortigate-end-of-support	2907
diagnose fortiguard-resources log fortiswitch-end-of-support	2907
diagnose fortiguard-resources log ips-information	2907
diagnose fortiguard-resources log maintainer	2907
diagnose fortiguard-resources log prefix-links	2908
diagnose fortiguard-resources log sprite-casb	2908
diagnose fortiguard-resources log sprite-isdb	2908

diagnose fortiguard-resources log sprite-map	2908
diagnose fortiguard-resources log static-links	2908
diagnose fortiguard-resources log wf-categories	2908
diagnose fortiguard-resources update	2909
diagnose fortiguard-resources update app-categories	2909
diagnose fortiguard-resources update app-info	2909
diagnose fortiguard-resources update dlp-object	2909
diagnose fortiguard-resources update fortiap-end-of-support	2909
diagnose fortiguard-resources update fortitender-end-of-support	2910
diagnose fortiguard-resources update fortigate-end-of-support	2910
diagnose fortiguard-resources update fortiswitch-end-of-support	2910
diagnose fortiguard-resources update ips-information	2910
diagnose fortiguard-resources update prefix-links	2910
diagnose fortiguard-resources update sprite-casb	2911
diagnose fortiguard-resources update sprite-isdb	2911
diagnose fortiguard-resources update sprite-map	2911
diagnose fortiguard-resources update static-links	2911
diagnose fortiguard-resources update wf-categories	2911
diagnose fortimq	2911
diagnose fortimq test	2912
diagnose fortism	2912
diagnose fortism domain	2912
diagnose fortism domain list	2912
diagnose fortitoken	2912
diagnose fortitoken debug	2913
diagnose fortitoken debug disable	2913
diagnose fortitoken debug enable	2913
diagnose fortitoken info	2913
diagnose fortitoken test	2913
diagnose fortitoken-cloud	2914
diagnose fortitoken-cloud clear	2914
diagnose fortitoken-cloud debug	2914
diagnose fortitoken-cloud debug disable	2915
diagnose fortitoken-cloud debug enable	2915
diagnose fortitoken-cloud debug info	2915
diagnose fortitoken-cloud delete	2915
diagnose fortitoken-cloud migrate-ftm	2915
diagnose fortitoken-cloud server	2916
diagnose fortitoken-cloud set-http	2916
diagnose fortitoken-cloud show	2916
diagnose fortitoken-cloud sync	2916
diagnose fortitoken-cloud update	2917
diagnose fortiview	2917
diagnose fortiview device	2917
diagnose fortiview result	2917
diagnose fortiview sortby	2918
diagnose fortiview time	2918
diagnose fortiview view	2918

diagnose geoip	2918
diagnose geoip delete-geoip-db	2918
diagnose geoip geoip-query	2918
diagnose geoip ip2country	2919
diagnose geoip iprange	2919
diagnose geoip iprange6	2919
diagnose hardware	2919
diagnose hardware certificate	2920
diagnose hardware deviceinfo	2920
diagnose hardware deviceinfo disk	2920
diagnose hardware deviceinfo nic	2920
diagnose hardware deviceinfo nic-channel	2921
diagnose hardware deviceinfo nic-stats	2921
diagnose hardware getcbp	2921
diagnose hardware ioport	2921
diagnose hardware ioport byte	2921
diagnose hardware ioport long	2921
diagnose hardware ioport word	2922
diagnose hardware lspci	2922
diagnose hardware mii	2922
diagnose hardware setcbp	2922
diagnose hardware setpci	2922
diagnose hardware sysinfo	2922
diagnose hardware sysinfo conserve	2923
diagnose hardware sysinfo cpu	2923
diagnose hardware sysinfo interrupts	2923
diagnose hardware sysinfo iomem	2923
diagnose hardware sysinfo ioports	2923
diagnose hardware sysinfo memory	2923
diagnose hardware sysinfo mtrr	2924
diagnose hardware sysinfo slab	2924
diagnose internet-service	2924
diagnose internet-service id	2924
diagnose internet-service id-summary	2924
diagnose internet-service info	2925
diagnose internet-service match	2925
diagnose internet-service sld	2925
diagnose internet-service status-read	2926
diagnose internet-service6	2926
diagnose internet-service6 id	2926
diagnose internet-service6 id-summary	2926
diagnose internet-service6 info	2926
diagnose internet-service6 match	2927
diagnose internet-service-name	2927
diagnose internet-service-name check-duplicate	2927
diagnose internet-service-name cleanup	2928
diagnose internet-service-name list	2928
diagnose ip address	2928
diagnose ip address add	2928

diagnose ip address delete	2929
diagnose ip address list	2929
diagnose ip arp	2929
diagnose ip arp add	2929
diagnose ip arp delete	2930
diagnose ip arp list	2930
diagnose ip gre-tunnel	2930
diagnose ip gre-tunnel list	2930
diagnose ip ipip-tunnel	2930
diagnose ip ipip-tunnel list	2931
diagnose ip multicast	2931
diagnose ip multicast get-igmp-limit	2931
diagnose ip multicast group-membership	2931
diagnose ip multicast mac	2931
diagnose ip multicast mfc-add	2932
diagnose ip multicast mfc-del	2932
diagnose ip multicast mfc-flush	2932
diagnose ip multicast mroute	2932
diagnose ip multicast status	2933
diagnose ip multicast vif	2933
diagnose ip parp	2933
diagnose ip parp list	2933
diagnose ip proute	2933
diagnose ip proute match	2933
diagnose ip route	2934
diagnose ip route add	2934
diagnose ip route delete	2935
diagnose ip route list	2935
diagnose ip route match	2935
diagnose ip route verify	2936
diagnose ip router bfd	2936
diagnose ip router bfd all	2937
diagnose ip router bfd cmdb	2937
diagnose ip router bfd events	2937
diagnose ip router bfd filter	2937
diagnose ip router bfd fsm	2937
diagnose ip router bfd nl	2937
diagnose ip router bfd packet	2938
diagnose ip router bfd show	2938
diagnose ip router bgp	2938
diagnose ip router bgp all	2938
diagnose ip router bgp dampening	2939
diagnose ip router bgp events	2939
diagnose ip router bgp filters	2939
diagnose ip router bgp fsm	2939
diagnose ip router bgp keepalives	2939
diagnose ip router bgp level	2939
diagnose ip router bgp level critical	2940

diagnose ip router bgp level error	2940
diagnose ip router bgp level info	2940
diagnose ip router bgp level none	2940
diagnose ip router bgp level warn	2940
diagnose ip router bgp nsm	2940
diagnose ip router bgp set-filter	2941
diagnose ip router bgp show	2941
diagnose ip router bgp updates	2941
diagnose ip router command	2941
diagnose ip router command show	2941
diagnose ip router command show-vrf	2941
diagnose ip router igmp	2942
diagnose ip router igmp all	2942
diagnose ip router igmp decode	2942
diagnose ip router igmp encode	2942
diagnose ip router igmp events	2943
diagnose ip router igmp fsm	2943
diagnose ip router igmp level	2943
diagnose ip router igmp level critical	2943
diagnose ip router igmp level error	2943
diagnose ip router igmp level info	2943
diagnose ip router igmp level none	2944
diagnose ip router igmp level warn	2944
diagnose ip router igmp show	2944
diagnose ip router igmp tib	2944
diagnose ip router isis	2944
diagnose ip router isis all	2945
diagnose ip router isis events	2945
diagnose ip router isis ifsm	2945
diagnose ip router isis level	2945
diagnose ip router isis level critical	2945
diagnose ip router isis level error	2945
diagnose ip router isis level info	2946
diagnose ip router isis level none	2946
diagnose ip router isis level warn	2946
diagnose ip router isis lsp	2946
diagnose ip router isis n fsm	2946
diagnose ip router isis nsm	2946
diagnose ip router isis pdu	2947
diagnose ip router isis show	2947
diagnose ip router isis spf	2947
diagnose ip router ospf	2947
diagnose ip router ospf all	2948
diagnose ip router ospf events	2948
diagnose ip router ospf ifsm	2948
diagnose ip router ospf level	2948
diagnose ip router ospf level critical	2948
diagnose ip router ospf level error	2948
diagnose ip router ospf level info	2949

diagnose ip router ospf level none	2949
diagnose ip router ospf level warn	2949
diagnose ip router ospf lsa	2949
diagnose ip router ospf nsm	2949
diagnose ip router ospf nsm	2949
diagnose ip router ospf packet	2950
diagnose ip router ospf route	2950
diagnose ip router ospf show	2950
diagnose ip router pim-dm	2950
diagnose ip router pim-dm all	2951
diagnose ip router pim-dm context	2951
diagnose ip router pim-dm decode	2951
diagnose ip router pim-dm encode	2951
diagnose ip router pim-dm fsm	2951
diagnose ip router pim-dm level	2951
diagnose ip router pim-dm level critical	2952
diagnose ip router pim-dm level error	2952
diagnose ip router pim-dm level info	2952
diagnose ip router pim-dm level none	2952
diagnose ip router pim-dm level warn	2952
diagnose ip router pim-dm mrt	2952
diagnose ip router pim-dm nexthop	2953
diagnose ip router pim-dm nsm	2953
diagnose ip router pim-dm show	2953
diagnose ip router pim-dm vif	2953
diagnose ip router pim-sm	2953
diagnose ip router pim-sm all	2954
diagnose ip router pim-sm events	2955
diagnose ip router pim-sm level	2955
diagnose ip router pim-sm level critical	2955
diagnose ip router pim-sm level error	2955
diagnose ip router pim-sm level info	2955
diagnose ip router pim-sm level none	2955
diagnose ip router pim-sm level warn	2956
diagnose ip router pim-sm mfc	2956
diagnose ip router pim-sm mib	2956
diagnose ip router pim-sm nexthop	2956
diagnose ip router pim-sm nsm	2956
diagnose ip router pim-sm packet	2956
diagnose ip router pim-sm packet all	2957
diagnose ip router pim-sm packet in	2957
diagnose ip router pim-sm packet out	2957
diagnose ip router pim-sm show	2957
diagnose ip router pim-sm state	2957
diagnose ip router pim-sm timer	2957
diagnose ip router pim-sm timer all	2958
diagnose ip router pim-sm timer assert	2958
diagnose ip router pim-sm timer assert all	2958
diagnose ip router pim-sm timer assert at	2958

diagnose ip router pim-sm timer bsr	2958
diagnose ip router pim-sm timer bsr all	2958
diagnose ip router pim-sm timer bsr bst	2959
diagnose ip router pim-sm timer bsr crp	2959
diagnose ip router pim-sm timer hello	2959
diagnose ip router pim-sm timer hello all	2959
diagnose ip router pim-sm timer hello ht	2959
diagnose ip router pim-sm timer hello nlt	2959
diagnose ip router pim-sm timer hello tht	2960
diagnose ip router pim-sm timer joinprune	2960
diagnose ip router pim-sm timer joinprune all	2960
diagnose ip router pim-sm timer joinprune et	2960
diagnose ip router pim-sm timer joinprune jt	2960
diagnose ip router pim-sm timer joinprune kat	2960
diagnose ip router pim-sm timer joinprune ot	2961
diagnose ip router pim-sm timer joinprune ppt	2961
diagnose ip router pim-sm timer register	2961
diagnose ip router pim-sm timer register all	2961
diagnose ip router pim-sm timer register rst	2961
diagnose ip router rip	2961
diagnose ip router rip all	2962
diagnose ip router rip events	2962
diagnose ip router rip level	2962
diagnose ip router rip level critical	2962
diagnose ip router rip level error	2962
diagnose ip router rip level info	2963
diagnose ip router rip level none	2963
diagnose ip router rip level warn	2963
diagnose ip router rip nsm	2963
diagnose ip router rip packet	2963
diagnose ip router rip show	2963
diagnose ip router zl	2964
diagnose ip router zl disable	2964
diagnose ip router zl enable	2964
diagnose ip router zl show	2964
diagnose ip rtcache	2964
diagnose ip rtcache stats	2964
diagnose ip tcp	2965
diagnose ip tcp list	2965
diagnose ip udp	2965
diagnose ip udp list	2965
diagnose ips anomaly	2965
diagnose ips anomaly clear	2966
diagnose ips anomaly config	2966
diagnose ips anomaly filter	2966
diagnose ips anomaly filter clear	2966
diagnose ips anomaly filter freq	2966
diagnose ips anomaly filter id	2967

diagnose ips anomaly filter ip	2967
diagnose ips anomaly filter pps	2967
diagnose ips anomaly list	2967
diagnose ips anomaly status	2968
diagnose ips anomaly6	2968
diagnose ips anomaly6 clear	2968
diagnose ips anomaly6 config	2968
diagnose ips anomaly6 filter	2968
diagnose ips anomaly6 filter clear	2969
diagnose ips anomaly6 filter freq	2969
diagnose ips anomaly6 filter id	2969
diagnose ips anomaly6 filter ip	2969
diagnose ips anomaly6 filter pps	2969
diagnose ips anomaly6 list	2970
diagnose ips anomaly6 status	2970
diagnose ips av avengine	2970
diagnose ips av avengine bypass-disable	2970
diagnose ips av avengine bypass-enable	2970
diagnose ips av avengine run-diagnose	2971
diagnose ips av cache	2971
diagnose ips av cache clear	2971
diagnose ips av cache delete	2971
diagnose ips av cache list	2971
diagnose ips av cache set-age	2972
diagnose ips av cache status	2972
diagnose ips av mode	2972
diagnose ips av mode show	2972
diagnose ips av query	2973
diagnose ips av query stats	2973
diagnose ips av query stats-clear	2973
diagnose ips av stats	2973
diagnose ips av stats clear	2973
diagnose ips av stats show	2973
diagnose ips av timeout	2974
diagnose ips av timeout set	2974
diagnose ips av timeout show	2974
diagnose ips config disable	2974
diagnose ips config disable log-verbose	2974
diagnose ips config enable	2975
diagnose ips config enable log-verbose	2975
diagnose ips dac	2975
diagnose ips dac clear	2975
diagnose ips dac info	2975
diagnose ips debug disable	2976
diagnose ips debug disable all	2977
diagnose ips debug disable av	2977
diagnose ips debug disable content	2977
diagnose ips debug disable content_detail	2977

diagnose ips debug disable dac	2977
diagnose ips debug disable detect	2977
diagnose ips debug disable diameter	2978
diagnose ips debug disable dissector	2978
diagnose ips debug disable dns	2978
diagnose ips debug disable error	2978
diagnose ips debug disable http	2978
diagnose ips debug disable im	2978
diagnose ips debug disable init	2979
diagnose ips debug disable ipsa	2979
diagnose ips debug disable log	2979
diagnose ips debug disable mail	2979
diagnose ips debug disable mime	2979
diagnose ips debug disable p2p	2979
diagnose ips debug disable packet	2980
diagnose ips debug disable packet_detail	2980
diagnose ips debug disable packet_dump	2980
diagnose ips debug disable parse	2980
diagnose ips debug disable proxy	2980
diagnose ips debug disable quic	2980
diagnose ips debug disable rpc	2981
diagnose ips debug disable sctp	2981
diagnose ips debug disable session	2981
diagnose ips debug disable smb	2981
diagnose ips debug disable ssh	2981
diagnose ips debug disable ssl	2981
diagnose ips debug disable state	2982
diagnose ips debug disable tcp	2982
diagnose ips debug disable timeout	2982
diagnose ips debug disable urlfilter	2982
diagnose ips debug disable voip	2982
diagnose ips debug disable warn	2982
diagnose ips debug enable	2983
diagnose ips debug enable all	2984
diagnose ips debug enable av	2984
diagnose ips debug enable content	2984
diagnose ips debug enable content_detail	2984
diagnose ips debug enable dac	2984
diagnose ips debug enable detect	2984
diagnose ips debug enable diameter	2985
diagnose ips debug enable dissector	2985
diagnose ips debug enable dns	2985
diagnose ips debug enable error	2985
diagnose ips debug enable http	2985
diagnose ips debug enable im	2985
diagnose ips debug enable init	2986
diagnose ips debug enable ipsa	2986
diagnose ips debug enable log	2986
diagnose ips debug enable mail	2986

diagnose ips debug enable mime	2986
diagnose ips debug enable ml	2986
diagnose ips debug enable p2p	2987
diagnose ips debug enable packet	2987
diagnose ips debug enable packet_detail	2987
diagnose ips debug enable packet_dump	2987
diagnose ips debug enable parse	2987
diagnose ips debug enable proxy	2987
diagnose ips debug enable quic	2988
diagnose ips debug enable rpc	2988
diagnose ips debug enable sctp	2988
diagnose ips debug enable session	2988
diagnose ips debug enable smb	2988
diagnose ips debug enable ssh	2988
diagnose ips debug enable ssl	2989
diagnose ips debug enable state	2989
diagnose ips debug enable tcp	2989
diagnose ips debug enable timeout	2989
diagnose ips debug enable urlfilter	2989
diagnose ips debug enable voip	2989
diagnose ips debug enable warn	2990
diagnose ips debug level	2990
diagnose ips debug level reset	2990
diagnose ips debug level save	2990
diagnose ips debug status	2990
diagnose ips debug status show	2990
diagnose ips debug timelimit	2991
diagnose ips debug timelimit set	2991
diagnose ips dissector	2991
diagnose ips dissector bypass	2991
diagnose ips dissector dump	2991
diagnose ips dissector list	2992
diagnose ips dissector status	2992
diagnose ips filter	2992
diagnose ips filter clear	2992
diagnose ips filter process_id	2992
diagnose ips filter set	2993
diagnose ips filter status	2993
diagnose ips filter timelimit	2993
diagnose ips global rule	2993
diagnose ips global rule reload	2993
diagnose ips gtp	2994
diagnose ips gtp clear	2994
diagnose ips gtp list	2994
diagnose ips gtp stats	2994
diagnose ips gtp stats-clear	2995
diagnose ips ipsa	2995
diagnose ips ipsa info	2995

diagnose ips ipsa read-ridmap	2995
diagnose ips l2ips	2995
diagnose ips l2ips stats	2995
diagnose ips memory	2996
diagnose ips memory compact	2996
diagnose ips memory profiling	2996
diagnose ips memory status	2996
diagnose ips memory track	2996
diagnose ips memory track-glibc	2997
diagnose ips memory track-print	2997
diagnose ips memory track-size	2997
diagnose ips packet	2997
diagnose ips packet clear	2998
diagnose ips packet status	2998
diagnose ips pme debug	2998
diagnose ips pme debug disable	2998
diagnose ips pme debug enable	2998
diagnose ips pme debug status	2999
diagnose ips pme debug verbose	2999
diagnose ips pme detail	2999
diagnose ips pme detail addr	2999
diagnose ips pme detail all	2999
diagnose ips pme detail auth	3000
diagnose ips pme detail def_port	3000
diagnose ips pme detail intf	3000
diagnose ips pme detail isdb	3000
diagnose ips pme detail none	3000
diagnose ips pme detail sched	3000
diagnose ips pme detail service	3001
diagnose ips pme dynamic-address	3001
diagnose ips pme dynamic-address list	3001
diagnose ips pme fabric-address	3001
diagnose ips pme fabric-address list	3001
diagnose ips pme policy	3002
diagnose ips pme policy clear-stats	3002
diagnose ips pme policy def_port	3002
diagnose ips pme policy list	3002
diagnose ips pme policy stats	3002
diagnose ips raw	3003
diagnose ips raw clear	3003
diagnose ips raw status	3003
diagnose ips session	3003
diagnose ips session clear	3003
diagnose ips session content	3004
diagnose ips session list	3004
diagnose ips session performance	3004
diagnose ips session status	3004
diagnose ips share	3004

diagnose ips share clear	3005
diagnose ips share list	3005
diagnose ips share pool	3005
diagnose ips shmopts	3005
diagnose ips shmopts disable	3005
diagnose ips shmopts list	3006
diagnose ips shmopts reset	3006
diagnose ips shmopts status	3006
diagnose ips signature	3006
diagnose ips signature cycle	3006
diagnose ips signature hit	3007
diagnose ips signature on-hold	3007
diagnose ips signature status	3007
diagnose ips ssl	3007
diagnose ips ssl bypass	3008
diagnose ips ssl cc-alg	3008
diagnose ips ssl ciphers	3008
diagnose ips ssl clear	3008
diagnose ips ssl debug	3008
diagnose ips ssl debug-status	3009
diagnose ips ssl noscan	3009
diagnose ips ssl resume	3009
diagnose ips ssl status	3009
diagnose ips tcp	3010
diagnose ips tcp clear	3010
diagnose ips tcp stats	3010
diagnose ips test	3010
diagnose ips test cmd	3010
diagnose ips urlfilter	3011
diagnose ips urlfilter clear	3011
diagnose ips urlfilter status	3011
diagnose ips vpatch	3011
diagnose ips vpatch fmwp-enable-all	3011
diagnose ips vpatch fmwp-reset	3012
diagnose ips vpatch fmwp-status	3012
diagnose ips vpatch ot-status	3012
diagnose ips vpatch query	3012
diagnose ipv6 address	3012
diagnose ipv6 address add	3013
diagnose ipv6 address anycast	3013
diagnose ipv6 address delete	3013
diagnose ipv6 address list	3013
diagnose ipv6 address multicast	3013
diagnose ipv6 devconf	3014
diagnose ipv6 devconf accept-dad	3014
diagnose ipv6 devconf disable_ipv6	3014
diagnose ipv6 gre-tunnel	3014
diagnose ipv6 gre-tunnel list	3015

diagnose ipv6 ipv6-tunnel	3015
diagnose ipv6 ipv6-tunnel list	3015
diagnose ipv6 multicast	3015
diagnose ipv6 multicast mroute	3015
diagnose ipv6 multicast status	3016
diagnose ipv6 multicast vif	3016
diagnose ipv6 neighbor-cache	3016
diagnose ipv6 neighbor-cache add	3016
diagnose ipv6 neighbor-cache delete	3016
diagnose ipv6 neighbor-cache flush	3017
diagnose ipv6 neighbor-cache list	3017
diagnose ipv6 proute	3017
diagnose ipv6 proute match	3017
diagnose ipv6 route	3018
diagnose ipv6 route list	3018
diagnose ipv6 router ospf	3018
diagnose ipv6 router ospf all	3019
diagnose ipv6 router ospf events	3019
diagnose ipv6 router ospf ifsm	3019
diagnose ipv6 router ospf level	3019
diagnose ipv6 router ospf level critical	3019
diagnose ipv6 router ospf level error	3019
diagnose ipv6 router ospf level info	3020
diagnose ipv6 router ospf level none	3020
diagnose ipv6 router ospf level warn	3020
diagnose ipv6 router ospf lsa	3020
diagnose ipv6 router ospf n fsm	3020
diagnose ipv6 router ospf nsm	3020
diagnose ipv6 router ospf packet	3021
diagnose ipv6 router ospf route	3021
diagnose ipv6 router ospf show	3021
diagnose ipv6 router pim-sm	3021
diagnose ipv6 router pim-sm all	3022
diagnose ipv6 router pim-sm events	3022
diagnose ipv6 router pim-sm level	3023
diagnose ipv6 router pim-sm level critical	3023
diagnose ipv6 router pim-sm level error	3023
diagnose ipv6 router pim-sm level info	3023
diagnose ipv6 router pim-sm level none	3023
diagnose ipv6 router pim-sm level warn	3023
diagnose ipv6 router pim-sm mfc	3024
diagnose ipv6 router pim-sm mib	3024
diagnose ipv6 router pim-sm nexthop	3024
diagnose ipv6 router pim-sm nsm	3024
diagnose ipv6 router pim-sm packet	3024
diagnose ipv6 router pim-sm packet all	3024
diagnose ipv6 router pim-sm packet in	3025
diagnose ipv6 router pim-sm packet out	3025

diagnose ipv6 router pim-sm show	3025
diagnose ipv6 router pim-sm state	3025
diagnose ipv6 router pim-sm timer	3025
diagnose ipv6 router pim-sm timer all	3025
diagnose ipv6 router pim-sm timer assert	3026
diagnose ipv6 router pim-sm timer assert all	3026
diagnose ipv6 router pim-sm timer assert at	3026
diagnose ipv6 router pim-sm timer bsr	3026
diagnose ipv6 router pim-sm timer bsr all	3026
diagnose ipv6 router pim-sm timer bsr bst	3026
diagnose ipv6 router pim-sm timer bsr crp	3027
diagnose ipv6 router pim-sm timer hello	3027
diagnose ipv6 router pim-sm timer hello all	3027
diagnose ipv6 router pim-sm timer hello ht	3027
diagnose ipv6 router pim-sm timer hello nlt	3027
diagnose ipv6 router pim-sm timer hello tht	3027
diagnose ipv6 router pim-sm timer joinprune	3028
diagnose ipv6 router pim-sm timer joinprune all	3028
diagnose ipv6 router pim-sm timer joinprune et	3028
diagnose ipv6 router pim-sm timer joinprune jt	3028
diagnose ipv6 router pim-sm timer joinprune kat	3028
diagnose ipv6 router pim-sm timer joinprune ot	3028
diagnose ipv6 router pim-sm timer joinprune ppt	3029
diagnose ipv6 router pim-sm timer register	3029
diagnose ipv6 router pim-sm timer register all	3029
diagnose ipv6 router pim-sm timer register rst	3029
diagnose ipv6 router rip	3029
diagnose ipv6 router rip all	3030
diagnose ipv6 router rip events	3030
diagnose ipv6 router rip level	3030
diagnose ipv6 router rip level critical	3030
diagnose ipv6 router rip level error	3030
diagnose ipv6 router rip level info	3030
diagnose ipv6 router rip level none	3031
diagnose ipv6 router rip level warn	3031
diagnose ipv6 router rip nsm	3031
diagnose ipv6 router rip packet	3031
diagnose ipv6 router rip show	3031
diagnose ipv6 router zl6	3031
diagnose ipv6 router zl6 disable	3032
diagnose ipv6 router zl6 enable	3032
diagnose ipv6 router zl6 show	3032
diagnose ipv6 sit-tunnel	3032
diagnose ipv6 sit-tunnel list	3032
diagnose l2vpn evpn	3032
diagnose l2vpn evpn all	3033
diagnose l2vpn evpn cmdb	3033
diagnose l2vpn evpn events	3033
diagnose l2vpn evpn fdb	3033

diagnose l2vpn evpn flush	3033
diagnose l2vpn evpn ha	3034
diagnose l2vpn evpn macip	3034
diagnose l2vpn evpn nl	3034
diagnose l2vpn evpn resync	3034
diagnose l2vpn evpn show	3034
diagnose l2vpn evpn zebos	3034
diagnose lldp	3035
diagnose lldp config	3035
diagnose lldp restart	3035
diagnose lldp rx	3036
diagnose lldp rx neighbor	3036
diagnose lldp rx neighbor clear	3036
diagnose lldp rx neighbor details	3036
diagnose lldp rx neighbor summary	3036
diagnose lldp rx port	3036
diagnose lldp rx port details	3037
diagnose lldp rx port neighbor	3037
diagnose lldp rx port neighbor clear	3037
diagnose lldp rx port neighbor details	3037
diagnose lldp rx port neighbor summary	3037
diagnose lldp rx port summary	3037
diagnose lldp stats	3038
diagnose lldp stats config	3038
diagnose lldp stats crash	3038
diagnose lldp stats manager	3038
diagnose lldp stats rxtx	3038
diagnose lldp tx	3038
diagnose lldp tx port	3039
diagnose lldp tx port details	3039
diagnose lldp tx port summary	3039
diagnose log	3039
diagnose log alertmail	3040
diagnose log alertmail authcode	3040
diagnose log alertmail test	3040
diagnose log check-empty	3040
diagnose log clear-kernel-stats	3040
diagnose log dummy-log	3041
diagnose log dummy-log fill	3041
diagnose log dummy-log remove	3041
diagnose log field-enum	3041
diagnose log field-list	3041
diagnose log kernel-stats	3041
diagnose log severity	3042
diagnose log show	3042
diagnose log stress-test	3042
diagnose log sub-category	3042
diagnose log test	3042
diagnose log test-text	3042

diagnose log wireless-controller	3043
diagnose netlink aggregate	3043
diagnose netlink aggregate list	3043
diagnose netlink aggregate list-active	3043
diagnose netlink aggregate name	3043
diagnose netlink aggregate port	3044
diagnose netlink backlog	3044
diagnose netlink backlog get	3044
diagnose netlink backlog set	3044
diagnose netlink brctl	3045
diagnose netlink brctl domain	3045
diagnose netlink brctl list	3045
diagnose netlink brctl name	3045
diagnose netlink device	3046
diagnose netlink device list	3046
diagnose netlink dstmac	3046
diagnose netlink dstmac flush	3046
diagnose netlink dstmac list	3046
diagnose netlink interface	3047
diagnose netlink interface clear	3047
diagnose netlink interface list	3047
diagnose netlink interface packet-rate	3047
diagnose netlink interface speed-test	3047
diagnose netlink interface speed-test-result	3048
diagnose netlink interface speed-test-result-clear	3048
diagnose netlink interface speed-test-tunnel	3048
diagnose netlink intf-class	3049
diagnose netlink intf-class list	3049
diagnose netlink intf-qdisc	3049
diagnose netlink intf-qdisc list	3049
diagnose netlink qlen	3049
diagnose netlink qlen get	3050
diagnose netlink qlen set	3050
diagnose netlink redundant	3050
diagnose netlink redundant list	3050
diagnose netlink redundant name	3051
diagnose nodejs	3051
diagnose nodejs health-check	3051
diagnose nodejs health-check ping	3051
diagnose nodejs logs	3052
diagnose nodejs logs delete	3052
diagnose nodejs logs list	3052
diagnose nodejs logs show	3052
diagnose nodejs logs show-all	3052
diagnose nodejs performance	3053
diagnose nodejs performance mass-ztna-event-logs	3053
diagnose nodejs process	3053
diagnose nodejs process restart	3053

diagnose oci	3053
diagnose oci pubkey	3053
diagnose on-demand-sniffer	3054
diagnose on-demand-sniffer delete-results	3054
diagnose on-demand-sniffer list	3054
diagnose on-demand-sniffer start	3054
diagnose on-demand-sniffer stop	3055
diagnose radiusd	3055
diagnose radiusd test	3055
diagnose report	3055
diagnose report clear-filter	3056
diagnose report dataset	3056
diagnose report filter	3056
diagnose report min-points	3056
diagnose report ondemand-table	3056
diagnose report sql	3056
diagnose report time	3057
diagnose report top-n	3057
diagnose report-runner	3057
diagnose report-runner clean	3057
diagnose report-runner trigger	3057
diagnose report-runner trigger security-rating-reports	3058
diagnose report-runner vuln-clean	3058
diagnose report-runner vuln-read	3058
diagnose report-runner-v2	3058
diagnose report-runner-v2 clean	3058
diagnose report-runner-v2 security-rating	3059
diagnose report-runner-v2 security-rating clean	3059
diagnose report-runner-v2 security-rating reset-trigger	3059
diagnose report-runner-v2 security-rating trigger	3059
diagnose report-runner-v2 security-rating trigger-check	3059
diagnose rso	3059
diagnose rso delete	3060
diagnose rso delete ip	3060
diagnose rso delete ip6	3060
diagnose rso query	3060
diagnose rso query carrier-endpoint	3061
diagnose rso query ip	3061
diagnose rso query ip6	3061
diagnose rso query rso-key	3061
diagnose rso resync	3062
diagnose rso resync fgcp	3062
diagnose rso resync fgsp	3062
diagnose saas	3062
diagnose saas reload	3063
diagnose saas show	3063
diagnose saas show apps	3063
diagnose saas show details	3063

diagnose saas show status	3063
diagnose settings	3063
diagnose settings info	3064
diagnose settings reset	3064
diagnose sladb	3064
diagnose sladb domain-list	3064
diagnose sladb protocol-list	3064
diagnose sladb target-list	3065
diagnose sniffer	3065
diagnose sniffer dpdk	3065
diagnose sniffer migsock	3066
diagnose sniffer migsock debug-trace	3066
diagnose sniffer migsock debug-trace disable	3066
diagnose sniffer migsock debug-trace enable	3067
diagnose sniffer migsock filter	3067
diagnose sniffer migsock ssl-trace	3067
diagnose sniffer migsock ssl-trace disable	3067
diagnose sniffer migsock ssl-trace enable	3067
diagnose sniffer migsock start	3067
diagnose sniffer migsock timestamp	3068
diagnose sniffer migsock timestamp disable	3068
diagnose sniffer migsock timestamp enable	3068
diagnose sniffer packet	3068
diagnose snmp ip	3069
diagnose snmp ip frags	3069
diagnose snmp ip icmp	3069
diagnose snmp ip ip	3070
diagnose snmp ip tcp	3070
diagnose snmp ip udp	3070
diagnose snmp ip6	3070
diagnose snmp ip6 frags	3070
diagnose snmp ip6 icmp6	3071
diagnose snmp ip6 ip6	3071
diagnose snmp ip6 udp6	3071
diagnose snmp net	3071
diagnose snmp net stat	3072
diagnose snmp trap	3072
diagnose snmp trap send	3072
diagnose switch-controller	3072
diagnose switch-controller flow-collector	3076
diagnose switch-controller flow-collector status	3076
diagnose switch-controller mac-cache	3076
diagnose switch-controller mac-cache filter	3076
diagnose switch-controller mac-cache filter clear	3076
diagnose switch-controller mac-cache filter intf-name	3076
diagnose switch-controller mac-cache filter mac	3077
diagnose switch-controller mac-cache filter vlan-id	3077
diagnose switch-controller mac-cache show	3077

diagnose switch-controller mac-device	3077
diagnose switch-controller mac-device cache	3077
diagnose switch-controller mac-device dynamic	3078
diagnose switch-controller mac-device nac	3078
diagnose switch-controller mac-device nac known	3078
diagnose switch-controller mac-device nac onboarding	3078
diagnose switch-controller nac-tag	3078
diagnose switch-controller nac-tag add	3078
diagnose switch-controller nac-tag delete	3079
diagnose switch-controller nac-tag get	3079
diagnose switch-controller restart-daemon	3079
diagnose switch-controller restart-daemon acd	3079
diagnose switch-controller restart-daemon swtpd	3079
diagnose switch-controller switch-info	3080
diagnose switch-controller switch-info 802.1X	3080
diagnose switch-controller switch-info 802.1X-dacl	3080
diagnose switch-controller switch-info acl-counters	3080
diagnose switch-controller switch-info arp-inspection	3081
diagnose switch-controller switch-info arp-inspection stats	3081
diagnose switch-controller switch-info arp-inspection stats-clear	3081
diagnose switch-controller switch-info bpdu-guard-status	3081
diagnose switch-controller switch-info dhcp-snooping	3082
diagnose switch-controller switch-info dhcp-snooping database	3082
diagnose switch-controller switch-info dhcp-snooping status	3082
diagnose switch-controller switch-info fan	3082
diagnose switch-controller switch-info flapguard	3082
diagnose switch-controller switch-info flapguard status	3083
diagnose switch-controller switch-info flow-tracking	3083
diagnose switch-controller switch-info flow-tracking flows	3083
diagnose switch-controller switch-info flow-tracking flows-raw	3083
diagnose switch-controller switch-info flow-tracking statistics	3084
diagnose switch-controller switch-info igmp-snooping	3084
diagnose switch-controller switch-info igmp-snooping group	3084
diagnose switch-controller switch-info igmp-snooping status	3084
diagnose switch-controller switch-info ip-source-guard	3085
diagnose switch-controller switch-info ip-source-guard hardware	3085
diagnose switch-controller switch-info lldp	3085
diagnose switch-controller switch-info lldp neighbors-detail	3085
diagnose switch-controller switch-info lldp neighbors-summary	3086
diagnose switch-controller switch-info lldp stats	3086
diagnose switch-controller switch-info loop-guard	3086
diagnose switch-controller switch-info mac-limit-violations	3086
diagnose switch-controller switch-info mac-limit-violations all	3087
diagnose switch-controller switch-info mac-limit-violations interface	3087
diagnose switch-controller switch-info mac-limit-violations vlan	3087
diagnose switch-controller switch-info mac-table	3087
diagnose switch-controller switch-info mclag	3088
diagnose switch-controller switch-info mclag icl	3088
diagnose switch-controller switch-info mclag list	3088

diagnose switch-controller switch-info mclag peer-consistency-check	3088
diagnose switch-controller switch-info mirror	3089
diagnose switch-controller switch-info mirror status	3089
diagnose switch-controller switch-info modules	3089
diagnose switch-controller switch-info modules detail	3089
diagnose switch-controller switch-info modules limits	3090
diagnose switch-controller switch-info modules status	3090
diagnose switch-controller switch-info modules summary	3090
diagnose switch-controller switch-info option82-mapping	3090
diagnose switch-controller switch-info option82-mapping snooping	3091
diagnose switch-controller switch-info option82-mapping snooping ascii	3091
diagnose switch-controller switch-info option82-mapping snooping hex	3091
diagnose switch-controller switch-info pdu-counters-list	3091
diagnose switch-controller switch-info poe	3092
diagnose switch-controller switch-info poe detail	3092
diagnose switch-controller switch-info poe summary	3092
diagnose switch-controller switch-info port-properties	3092
diagnose switch-controller switch-info port-stats	3093
diagnose switch-controller switch-info qos-stats	3093
diagnose switch-controller switch-info rpvst	3093
diagnose switch-controller switch-info status	3093
diagnose switch-controller switch-info stp	3094
diagnose switch-controller switch-info trunk	3094
diagnose switch-controller switch-info trunk config	3094
diagnose switch-controller switch-info trunk status	3094
diagnose switch-controller switch-recommendation	3095
diagnose switch-controller switch-recommendation bios-compatibility-check	3095
diagnose switch-controller switch-recommendation check-fortilink-link-redundancy	3095
diagnose switch-controller switch-recommendation check-isl-icl-link-redundancy	3095
diagnose switch-controller switch-recommendation check-isl-link-redundancy	3096
diagnose switch-controller switch-recommendation clear-dhcp-opt43-key	3096
diagnose switch-controller switch-recommendation config-dhcp-opt43-key	3097
diagnose switch-controller switch-recommendation disable-auto-config-poe-status	3097
diagnose switch-controller switch-recommendation disable-bounce-quarantine-link	3097
diagnose switch-controller switch-recommendation disable-poe-pre-standard-detection	3097
diagnose switch-controller switch-recommendation disable-stp-state-topology	3098
diagnose switch-controller switch-recommendation enable-auto-config-poe-status	3098
diagnose switch-controller switch-recommendation enable-bounce-quarantine-link	3098
diagnose switch-controller switch-recommendation enable-poe-pre-	3098

standard-detection	
diagnose switch-controller switch-recommendation enable-stp-state-topology	3099
diagnose switch-controller switch-recommendation fabric-lockdown-check	3099
diagnose switch-controller switch-recommendation fabric-lockdown-disable	3099
diagnose switch-controller switch-recommendation fabric-lockdown-enable	3100
diagnose switch-controller switch-recommendation get-mclag-tier1-candidate	3100
diagnose switch-controller switch-recommendation get-mclag-tier2-candidate	3100
diagnose switch-controller switch-recommendation get-mclag-tier3-candidate	3101
diagnose switch-controller switch-recommendation is-fortilink-capacity-exceeded	3101
diagnose switch-controller switch-recommendation is-switch-dual-homed	3101
diagnose switch-controller switch-recommendation lock-down-topo-lldp-profile	3102
diagnose switch-controller switch-recommendation pse-check	3102
diagnose switch-controller switch-recommendation pse-config	3102
diagnose switch-controller switch-recommendation set-tier-plus-mclag-icl	3103
diagnose switch-controller switch-recommendation set-tier1-mclag-icl	3103
diagnose switch-controller switch-recommendation tunnel-mode-settings	3103
diagnose switch-controller switch-recommendation unlock-topo-lldp-profile	3104
diagnose switch-controller system-info	3104
diagnose switch-controller system-info show	3104
diagnose switch-controller telemetry	3104
diagnose switch-controller telemetry show	3104
diagnose switch-controller telemetry show mac-stats	3105
diagnose switch-controller telemetry show mac-stats switch	3105
diagnose switch-controller telemetry show switch	3105
diagnose switch-controller telemetry show switch-port	3105
diagnose switch-controller topology	3106
diagnose switch-controller topology reset	3106
diagnose switch-controller topology reset fortilink-flag	3106
diagnose switch-controller topology reset isl-peer-flag	3106
diagnose switch-controller topology set	3106
diagnose switch-controller topology set fortilink-flag	3107
diagnose switch-controller topology set isl-peer-flag	3107
diagnose switch-controller traffic-capture	3107
diagnose switch-controller traffic-capture show	3107
diagnose switch-controller traffic-capture start	3107
diagnose switch-controller traffic-capture stop	3108
diagnose switch-controller trigger	3108
diagnose switch-controller trigger config-sync	3108
diagnose switch-controller trigger mac-sync	3108
diagnose switch-controller trigger nac-mac-cache-sync	3109
diagnose switch-controller trigger reset-hardware-counters	3109
diagnose switch-controller trigger restore-hardware-counters	3109

diagnose switch-controller tunnel-status	3109
diagnose sys	3110
diagnose sys acme	3135
diagnose sys acme add-account	3135
diagnose sys acme clear-staging	3135
diagnose sys acme debug	3136
diagnose sys acme debug disable	3136
diagnose sys acme debug enable	3136
diagnose sys acme debug enable level	3136
diagnose sys acme debug enable level debug	3136
diagnose sys acme debug enable level error	3136
diagnose sys acme debug enable level info	3137
diagnose sys acme debug enable level verbose	3137
diagnose sys acme debug enable level veryverbose	3137
diagnose sys acme debug enable level warning	3137
diagnose sys acme delete-cert	3137
diagnose sys acme force-renew	3137
diagnose sys acme list-archive	3138
diagnose sys acme list-domains	3138
diagnose sys acme purge-all	3138
diagnose sys acme purge-archive	3138
diagnose sys acme purge-certs	3138
diagnose sys acme regenerate-client-config	3138
diagnose sys acme regenerate-store	3139
diagnose sys acme restart	3139
diagnose sys acme show-archive	3139
diagnose sys acme show-client-config	3139
diagnose sys acme show-passphrase	3139
diagnose sys acme status-full	3139
diagnose sys botnet-domain	3140
diagnose sys botnet-domain hit	3140
diagnose sys botnet-domain list	3140
diagnose sys botnet-ip	3140
diagnose sys botnet-ip find	3140
diagnose sys botnet-ip flush	3141
diagnose sys botnet-ip hit	3141
diagnose sys botnet-ip list	3141
diagnose sys certificate-blocklist	3141
diagnose sys certificate-blocklist count	3141
diagnose sys certificate-blocklist delete-mcdb	3142
diagnose sys certificate-blocklist query	3142
diagnose sys certificate-blocklist read-range	3142
diagnose sys certificate-blocklist status	3142
diagnose sys cmdb	3142
diagnose sys cmdb buf-sz	3143
diagnose sys cmdb dump	3143
diagnose sys cmdb dump vdom	3143
diagnose sys cmdb flag	3143
diagnose sys cmdb flag info	3143

diagnose sys cmdb flag reset	3143
diagnose sys cmdb flag reset script-running	3144
diagnose sys cmdb info	3144
diagnose sys cmdb obj-verno	3144
diagnose sys cmdb refcnt	3144
diagnose sys cmdb refcnt reset	3144
diagnose sys cmdb refcnt show	3145
diagnose sys cmdb set-readlock	3145
diagnose sys cmdb unset-readlock	3145
diagnose sys cmdb-profile	3145
diagnose sys cmdb-profile info	3145
diagnose sys cmdb-profile node	3145
diagnose sys cmdb-profile reset	3146
diagnose sys cmdb-profile top10	3146
diagnose sys cmdb-profile top10 average	3146
diagnose sys cmdb-profile top10 total	3146
diagnose sys config-transaction	3146
diagnose sys config-transaction show	3147
diagnose sys config-transaction show entity-by-txn	3147
diagnose sys config-transaction show mctx	3147
diagnose sys config-transaction show txn-cli-commands	3147
diagnose sys config-transaction show txn-entity	3147
diagnose sys config-transaction show txn-info	3148
diagnose sys config-transaction show txn-lock	3148
diagnose sys config-transaction show txn-meta	3148
diagnose sys config-transaction status	3148
diagnose sys cpuset	3148
diagnose sys cpuset interrupt	3148
diagnose sys cpuset process	3149
diagnose sys csf	3149
diagnose sys csf authorization	3149
diagnose sys csf authorization accept	3149
diagnose sys csf authorization deny	3149
diagnose sys csf authorization pending-list	3150
diagnose sys csf downstream	3150
diagnose sys csf downstream-devices	3150
diagnose sys csf dynamic-sync-read	3150
diagnose sys csf dynamic-sync-request	3151
diagnose sys csf dynamic-sync-update	3151
diagnose sys csf fabric-device	3151
diagnose sys csf fabric-device list	3151
diagnose sys csf file	3151
diagnose sys csf file cat	3152
diagnose sys csf file top-mem	3152
diagnose sys csf forticloud-id-list	3152
diagnose sys csf get-bulk-global-view	3152
diagnose sys csf global	3152
diagnose sys csf initialize-cmd	3153
diagnose sys csf merge-cmd	3153

diagnose sys csf neighbor	3153
diagnose sys csf neighbor flush	3153
diagnose sys csf neighbor list	3154
diagnose sys csf query	3154
diagnose sys csf ratelimit-test-sender	3154
diagnose sys csf ratelimit-test-server	3154
diagnose sys csf send-test-log-upstream	3155
diagnose sys csf seqpacket-message-listener	3155
diagnose sys csf seqpacket-message-sender	3155
diagnose sys csf stream-message-listener	3155
diagnose sys csf stream-message-sender	3156
diagnose sys csf trigger-info-update	3156
diagnose sys csf tunnel-test-listener	3156
diagnose sys csf tunnel-test-sender	3156
diagnose sys csf upstream	3157
diagnose sys csf versions	3157
diagnose sys csum	3157
diagnose sys dayst-info	3157
diagnose sys device	3157
diagnose sys device add	3158
diagnose sys device delete	3158
diagnose sys device list	3158
diagnose sys dump-conserve-info	3158
diagnose sys emac-vlan	3158
diagnose sys emac-vlan fdb	3159
diagnose sys emac-vlan fdb list	3159
diagnose sys emac-vlan stat	3159
diagnose sys external-address-resource	3159
diagnose sys external-address-resource list	3159
diagnose sys external-generic-address-resource	3160
diagnose sys external-generic-address-resource remove-by-name	3160
diagnose sys external-generic-address-resource remove-by-namespace	3160
diagnose sys external-mac-resource	3160
diagnose sys external-mac-resource list	3161
diagnose sys external-resource	3161
diagnose sys external-resource list	3161
diagnose sys external-resource push-add	3161
diagnose sys external-resource push-api-json-commands	3161
diagnose sys external-resource push-remove	3162
diagnose sys external-resource push-snapshot	3162
diagnose sys external-resource stats	3162
diagnose sys filesystem	3162
diagnose sys filesystem hash	3162
diagnose sys filesystem last-modified-files	3162
diagnose sys filesystem lsof	3163
diagnose sys filesystem open-files	3163
diagnose sys filesystem tree	3163
diagnose sys fips	3163
diagnose sys fips error-mode	3164

diagnose sys fips kat-error	3164
diagnose sys flash	3164
diagnose sys flash format	3164
diagnose sys flash list	3164
diagnose sys forticonverter	3165
diagnose sys forticonverter available-source-devices	3165
diagnose sys forticonverter create-ticket	3165
diagnose sys forticonverter custom-create-ticket	3165
diagnose sys forticonverter download-status	3165
diagnose sys forticonverter eligibility-status	3166
diagnose sys forticonverter get-prompt-visibility	3166
diagnose sys forticonverter result-availability	3166
diagnose sys forticonverter set-source-fortigate	3166
diagnose sys forticonverter source-config-upload-status	3167
diagnose sys forticonverter source-interfaces	3167
diagnose sys forticonverter start-download	3167
diagnose sys forticonverter submitted-info	3167
diagnose sys forticonverter update-eligibility	3168
diagnose sys forticonverter update-result-availability	3168
diagnose sys forticonverter upload-local-config	3168
diagnose sys forticonverter upload-status	3168
diagnose sys frag-mem	3168
diagnose sys fullcone	3169
diagnose sys geneve	3169
diagnose sys geneve list	3169
diagnose sys geneve stat	3169
diagnose sys gre	3169
diagnose sys gre keepalive	3169
diagnose sys gre list	3170
diagnose sys h323	3170
diagnose sys h323 call	3170
diagnose sys h323 call list	3170
diagnose sys h323 debug-mask	3170
diagnose sys h323 peer	3170
diagnose sys h323 peer list	3171
diagnose sys h323 status	3171
diagnose sys ha	3171
diagnose sys ha autoscale-peers	3171
diagnose sys ha check-vc	3171
diagnose sys ha checksum	3171
diagnose sys ha checksum autoscale-cluster	3172
diagnose sys ha checksum cached	3172
diagnose sys ha checksum cluster	3172
diagnose sys ha checksum log	3172
diagnose sys ha checksum log clear	3172
diagnose sys ha checksum log disable	3173
diagnose sys ha checksum log enable	3173
diagnose sys ha checksum recalculate	3173
diagnose sys ha checksum show	3173

diagnose sys ha checksum show-nonsync	3174
diagnose sys ha checksum test	3174
diagnose sys ha dump-by	3174
diagnose sys ha dump-by debug-zone	3174
diagnose sys ha dump-by device	3174
diagnose sys ha dump-by group	3174
diagnose sys ha dump-by kernel	3175
diagnose sys ha dump-by rcache	3175
diagnose sys ha dump-by vcluster	3175
diagnose sys ha dump-by vdom	3175
diagnose sys ha extfile-sig	3175
diagnose sys ha fgsp-zone	3175
diagnose sys ha fib	3176
diagnose sys ha hactx-stats	3176
diagnose sys ha hactx-stats clear	3176
diagnose sys ha hadiff	3176
diagnose sys ha hadiff log	3176
diagnose sys ha hadiff log clear	3176
diagnose sys ha hadiff log disable	3177
diagnose sys ha hadiff log enable	3177
diagnose sys ha hadiff max-sync-turns	3177
diagnose sys ha hadiff max-unsync-wait	3177
diagnose sys ha hadiff status	3177
diagnose sys ha hadiff sync-from-higher	3178
diagnose sys ha hasync-conn-max-buf	3178
diagnose sys ha hasync-stats	3178
diagnose sys ha hasync-stats all	3178
diagnose sys ha hasync-stats by-object	3178
diagnose sys ha hasync-stats most-recent	3179
diagnose sys ha hasync-stats most-time	3179
diagnose sys ha heartbeat	3179
diagnose sys ha history	3179
diagnose sys ha history clear	3179
diagnose sys ha history read	3180
diagnose sys ha mac	3180
diagnose sys ha pingsvr-secondary-force-reset	3180
diagnose sys ha recalculate-extfile-signature	3180
diagnose sys ha reset-health-status	3180
diagnose sys ha reset-uptime	3180
diagnose sys ha reset-uptime-primary-only	3181
diagnose sys ha session-sync-dev	3181
diagnose sys ha session-sync-dev clear	3181
diagnose sys ha session-sync-dev set	3181
diagnose sys ha standalone-peers	3181
diagnose sys ha standalone-peers reset-stats	3181
diagnose sys ha stats	3182
diagnose sys ha status	3182
diagnose sys ha sync-stats	3182
diagnose sys ha sync-stats-reset	3182

diagnose sys ha vlan-hb-monitor	3182
diagnose sys icap-remote-server	3182
diagnose sys icap-remote-server status	3183
diagnose sys icb	3183
diagnose sys icb debug	3183
diagnose sys icb debug disable	3183
diagnose sys icb debug info	3183
diagnose sys icb debug show	3183
diagnose sys icb debug verbose	3184
diagnose sys icb stats	3184
diagnose sys icb stats list	3184
diagnose sys icb status	3184
diagnose sys icb status current	3184
diagnose sys iotop	3184
diagnose sys ipam	3185
diagnose sys ipam delete	3185
diagnose sys ipam delete device	3185
diagnose sys ipam largest-available-subnet	3185
diagnose sys ipam list	3185
diagnose sys ipam list entries	3185
diagnose sys ipam list free-subnets	3186
diagnose sys ipsec-aggregate	3186
diagnose sys ipsec-aggregate list	3186
diagnose sys kill	3186
diagnose sys link-monitor	3186
diagnose sys link-monitor filter	3187
diagnose sys link-monitor filter clear	3187
diagnose sys link-monitor filter name	3187
diagnose sys link-monitor interface	3187
diagnose sys link-monitor launch	3187
diagnose sys link-monitor reset-monitor	3188
diagnose sys link-monitor sdwan-hc	3188
diagnose sys link-monitor sdwan-service	3188
diagnose sys link-monitor shm-band-stats	3188
diagnose sys link-monitor shm-stats	3189
diagnose sys link-monitor status	3189
diagnose sys link-monitor tunnel	3189
diagnose sys link-monitor zone-intf	3189
diagnose sys link-monitor-passive	3190
diagnose sys link-monitor-passive admin	3190
diagnose sys link-monitor-passive admin dbg-rpt	3190
diagnose sys link-monitor-passive admin dbg-rpt reset	3190
diagnose sys link-monitor-passive admin dbg-rpt retrans	3190
diagnose sys link-monitor-passive admin dbg-rpt rtt	3191
diagnose sys link-monitor-passive admin dbg-rpt syn-retrans	3191
diagnose sys link-monitor-passive admin delete	3192
diagnose sys link-monitor-passive admin flush	3192
diagnose sys link-monitor-passive admin list	3192
diagnose sys link-monitor-passive admin list by-application	3193

diagnose sys link-monitor-passive admin list by-interface	3193
diagnose sys link-monitor-passive agent	3193
diagnose sys link-monitor-passive agent agent-oif-map	3193
diagnose sys link-monitor-passive agent flush	3193
diagnose sys link-monitor-passive agent flush-app	3194
diagnose sys link-monitor-passive agent list	3194
diagnose sys link-monitor-passive agent list-app	3194
diagnose sys link-monitor-passive agent send-report	3194
diagnose sys link-monitor-passive remote	3195
diagnose sys link-monitor-passive remote list	3195
diagnose sys logdisk	3195
diagnose sys logdisk purge-log-data	3195
diagnose sys logdisk quota	3195
diagnose sys logdisk smart	3195
diagnose sys logdisk status	3196
diagnose sys logdisk status monitor	3196
diagnose sys logdisk usage	3196
diagnose sys mcast-session	3196
diagnose sys mcast-session clear	3196
diagnose sys mcast-session filter	3196
diagnose sys mcast-session filter clear	3197
diagnose sys mcast-session filter clear dport	3197
diagnose sys mcast-session filter clear dst	3197
diagnose sys mcast-session filter clear proto	3197
diagnose sys mcast-session filter clear sintf	3197
diagnose sys mcast-session filter clear sport	3197
diagnose sys mcast-session filter clear src	3198
diagnose sys mcast-session filter clear vd	3198
diagnose sys mcast-session filter dport	3198
diagnose sys mcast-session filter dst	3198
diagnose sys mcast-session filter negate	3198
diagnose sys mcast-session filter negate dport	3199
diagnose sys mcast-session filter negate dst	3199
diagnose sys mcast-session filter negate proto	3199
diagnose sys mcast-session filter negate sintf	3199
diagnose sys mcast-session filter negate sport	3199
diagnose sys mcast-session filter negate src	3199
diagnose sys mcast-session filter negate vd	3200
diagnose sys mcast-session filter proto	3200
diagnose sys mcast-session filter sintf	3200
diagnose sys mcast-session filter sport	3200
diagnose sys mcast-session filter src	3200
diagnose sys mcast-session filter vd	3201
diagnose sys mcast-session list	3201
diagnose sys mcast-session stat	3201
diagnose sys mcast-session6	3201
diagnose sys mcast-session6 clear	3201
diagnose sys mcast-session6 filter	3202
diagnose sys mcast-session6 filter clear	3202

diagnose sys mcast-session6 filter clear dport	3202
diagnose sys mcast-session6 filter clear dst	3202
diagnose sys mcast-session6 filter clear proto	3202
diagnose sys mcast-session6 filter clear sintf	3202
diagnose sys mcast-session6 filter clear sport	3203
diagnose sys mcast-session6 filter clear src	3203
diagnose sys mcast-session6 filter clear vd	3203
diagnose sys mcast-session6 filter dport	3203
diagnose sys mcast-session6 filter dst	3203
diagnose sys mcast-session6 filter negate	3204
diagnose sys mcast-session6 filter negate dport	3204
diagnose sys mcast-session6 filter negate dst	3204
diagnose sys mcast-session6 filter negate proto	3204
diagnose sys mcast-session6 filter negate sintf	3204
diagnose sys mcast-session6 filter negate sport	3204
diagnose sys mcast-session6 filter negate src	3205
diagnose sys mcast-session6 filter negate vd	3205
diagnose sys mcast-session6 filter proto	3205
diagnose sys mcast-session6 filter sintf	3205
diagnose sys mcast-session6 filter sport	3205
diagnose sys mcast-session6 filter src	3206
diagnose sys mcast-session6 filter vd	3206
diagnose sys mcast-session6 list	3206
diagnose sys mcast-session6 stat	3206
diagnose sys mpstat	3207
diagnose sys ntp	3207
diagnose sys ntp status	3207
diagnose sys pair	3207
diagnose sys platform	3207
diagnose sys platform info	3207
diagnose sys print-conserve-info	3208
diagnose sys process	3208
diagnose sys process daemon-auto-restart	3208
diagnose sys process dump	3208
diagnose sys process nameof	3208
diagnose sys process pidof	3209
diagnose sys process pstack	3209
diagnose sys process sock-mem	3209
diagnose sys process socket	3209
diagnose sys process trace	3209
diagnose sys profile	3210
diagnose sys profile cpumask	3210
diagnose sys profile module	3210
diagnose sys profile show	3210
diagnose sys profile show detail	3210
diagnose sys profile show order	3210
diagnose sys profile start	3211
diagnose sys profile step	3211
diagnose sys profile stop	3211

diagnose sys profile sysmap	3211
diagnose sys proxy	3211
diagnose sys proxy bypass	3211
diagnose sys proxy bypass clear	3212
diagnose sys proxy bypass disable	3212
diagnose sys proxy bypass disable category	3212
diagnose sys proxy bypass disable category all	3212
diagnose sys proxy bypass disable category scanunit-submission	3212
diagnose sys proxy bypass disable category ssl	3212
diagnose sys proxy bypass disable category utm	3213
diagnose sys proxy bypass disable protocol	3213
diagnose sys proxy bypass disable protocol all	3213
diagnose sys proxy bypass disable protocol ftp	3213
diagnose sys proxy bypass disable protocol imap	3213
diagnose sys proxy bypass disable protocol nntp	3213
diagnose sys proxy bypass disable protocol pop3	3214
diagnose sys proxy bypass disable protocol smtp	3214
diagnose sys proxy bypass enable	3214
diagnose sys proxy bypass enable category	3214
diagnose sys proxy bypass enable category all	3214
diagnose sys proxy bypass enable category scanunit-submission	3214
diagnose sys proxy bypass enable category ssl	3215
diagnose sys proxy bypass enable category utm	3215
diagnose sys proxy bypass enable protocol	3215
diagnose sys proxy bypass enable protocol all	3215
diagnose sys proxy bypass enable protocol ftp	3215
diagnose sys proxy bypass enable protocol imap	3215
diagnose sys proxy bypass enable protocol nntp	3216
diagnose sys proxy bypass enable protocol pop3	3216
diagnose sys proxy bypass enable protocol smtp	3216
diagnose sys proxy bypass show	3216
diagnose sys proxy certificate-blocklist	3216
diagnose sys proxy certificate-blocklist flush	3216
diagnose sys proxy certificate-blocklist status	3217
diagnose sys proxy debug-filter	3217
diagnose sys proxy debug-filter clear	3217
diagnose sys proxy debug-filter list	3217
diagnose sys proxy debug-filter src	3217
diagnose sys proxy filter	3217
diagnose sys proxy filter clear	3218
diagnose sys proxy filter list	3218
diagnose sys proxy filter negate	3218
diagnose sys proxy filter negate vd	3218
diagnose sys proxy filter negate worker	3218
diagnose sys proxy filter vd	3218
diagnose sys proxy filter worker	3219
diagnose sys proxy log	3219
diagnose sys proxy log filter	3219
diagnose sys proxy log filter clear	3219

diagnose sys proxy log filter list	3219
diagnose sys proxy log filter negate	3219
diagnose sys proxy log filter negate vd	3220
diagnose sys proxy log filter negate worker	3220
diagnose sys proxy log filter vd	3220
diagnose sys proxy log filter worker	3220
diagnose sys proxy log-debug	3220
diagnose sys proxy memory	3221
diagnose sys proxy memory allocator	3221
diagnose sys proxy memory conserve	3221
diagnose sys proxy memory conserve enter	3221
diagnose sys proxy memory conserve exit	3221
diagnose sys proxy memory jemalloc	3221
diagnose sys proxy memory malloc	3222
diagnose sys proxy memory usage	3222
diagnose sys proxy restart	3222
diagnose sys proxy simulate-error	3222
diagnose sys proxy simulate-error scan-drop	3222
diagnose sys proxy simulate-error scan-drop disable	3222
diagnose sys proxy simulate-error scan-drop enable	3223
diagnose sys proxy simulate-error status	3223
diagnose sys proxy socket-options	3223
diagnose sys proxy socket-options linger	3223
diagnose sys proxy socket-options linger disable	3223
diagnose sys proxy socket-options linger enable	3223
diagnose sys proxy socket-options nagle	3224
diagnose sys proxy socket-options nagle disable	3224
diagnose sys proxy socket-options nagle enable	3224
diagnose sys proxy socket-options status	3224
diagnose sys proxy ssl	3224
diagnose sys proxy ssl bypass	3224
diagnose sys proxy ssl bypass flush	3225
diagnose sys proxy ssl bypass list	3225
diagnose sys proxy ssl crypto	3225
diagnose sys proxy ssl crypto async	3225
diagnose sys proxy ssl crypto sync	3225
diagnose sys proxy ssl exempt	3225
diagnose sys proxy ssl exempt flush	3226
diagnose sys proxy ssl exempt list	3226
diagnose sys proxy ssl rsa-blinding	3226
diagnose sys proxy ssl rsa-blinding off	3226
diagnose sys proxy ssl rsa-blinding on	3226
diagnose sys proxy ssl session	3226
diagnose sys proxy stats	3227
diagnose sys proxy stats all	3227
diagnose sys proxy stats clear	3227
diagnose sys proxy stats debug	3227
diagnose sys proxy stats list	3227
diagnose sys proxy stats protocol	3227

diagnose sys proxy stats vdom	3228
diagnose sys proxy stats vdom all	3228
diagnose sys proxy stats vdom list	3228
diagnose sys proxy stats vdom summary	3228
diagnose sys proxy valgrind	3228
diagnose sys proxy valgrind disable	3228
diagnose sys proxy valgrind enable	3229
diagnose sys proxy valgrind log	3229
diagnose sys proxy valgrind log clear	3229
diagnose sys proxy valgrind log show	3229
diagnose sys proxy valgrind memcheck	3229
diagnose sys proxy valgrind memcheck_less	3229
diagnose sys proxy valgrind status	3230
diagnose sys ptp	3230
diagnose sys ptp status	3230
diagnose sys route_tag	3230
diagnose sys route_tag flush	3230
diagnose sys route_tag list	3230
diagnose sys route_tag summary	3231
diagnose sys saml	3231
diagnose sys saml metadata	3231
diagnose sys scanunit	3231
diagnose sys scanunit auto-restart	3231
diagnose sys scanunit auto-restart requests	3231
diagnose sys scanunit auto-restart reset	3232
diagnose sys scanunit auto-restart status	3232
diagnose sys scanunit auto-restart time	3232
diagnose sys scanunit av	3232
diagnose sys scanunit av filetype-reuse	3232
diagnose sys scanunit av filetype-reuse disable	3233
diagnose sys scanunit av filetype-reuse enable	3233
diagnose sys scanunit av reload-avdb	3233
diagnose sys scanunit av reload-aveng	3233
diagnose sys scanunit av reload-fsa-ext	3233
diagnose sys scanunit bypass	3233
diagnose sys scanunit bypass clear	3234
diagnose sys scanunit bypass disable	3234
diagnose sys scanunit bypass disable category	3234
diagnose sys scanunit bypass disable category all	3234
diagnose sys scanunit bypass disable category av-engine	3234
diagnose sys scanunit bypass disable category scanunit	3234
diagnose sys scanunit bypass disable protocol	3235
diagnose sys scanunit bypass disable protocol all	3235
diagnose sys scanunit bypass disable protocol cifs	3235
diagnose sys scanunit bypass disable protocol ftp	3235
diagnose sys scanunit bypass disable protocol http	3235
diagnose sys scanunit bypass disable protocol imap	3235
diagnose sys scanunit bypass disable protocol nntp	3236
diagnose sys scanunit bypass disable protocol pop3	3236

diagnose sys scanunit bypass disable protocol smtp	3236
diagnose sys scanunit bypass enable	3236
diagnose sys scanunit bypass enable category	3236
diagnose sys scanunit bypass enable category all	3236
diagnose sys scanunit bypass enable category av-engine	3237
diagnose sys scanunit bypass enable category scanunit	3237
diagnose sys scanunit bypass enable protocol	3237
diagnose sys scanunit bypass enable protocol all	3237
diagnose sys scanunit bypass enable protocol cifs	3237
diagnose sys scanunit bypass enable protocol ftp	3237
diagnose sys scanunit bypass enable protocol http	3238
diagnose sys scanunit bypass enable protocol imap	3238
diagnose sys scanunit bypass enable protocol nntp	3238
diagnose sys scanunit bypass enable protocol pop3	3238
diagnose sys scanunit bypass enable protocol smtp	3238
diagnose sys scanunit bypass show	3238
diagnose sys scanunit cfg	3239
diagnose sys scanunit cfg clear	3239
diagnose sys scanunit cfg list	3239
diagnose sys scanunit crash-dump	3239
diagnose sys scanunit crash-dump clear	3239
diagnose sys scanunit crash-dump disable	3239
diagnose sys scanunit crash-dump enable	3240
diagnose sys scanunit crash-dump read	3240
diagnose sys scanunit debug	3240
diagnose sys scanunit debug all	3240
diagnose sys scanunit debug analytics	3240
diagnose sys scanunit debug antisipam	3241
diagnose sys scanunit debug daemon	3241
diagnose sys scanunit debug dlp	3241
diagnose sys scanunit debug fhl	3241
diagnose sys scanunit debug file-filter	3241
diagnose sys scanunit debug icb	3242
diagnose sys scanunit debug job	3242
diagnose sys scanunit debug level	3242
diagnose sys scanunit debug level error	3242
diagnose sys scanunit debug level info	3242
diagnose sys scanunit debug level verbose	3243
diagnose sys scanunit debug level warning	3243
diagnose sys scanunit debug outbreak-prevention	3243
diagnose sys scanunit debug quarantine	3243
diagnose sys scanunit debug reset	3243
diagnose sys scanunit debug sane	3244
diagnose sys scanunit debug show	3244
diagnose sys scanunit debug start	3244
diagnose sys scanunit debug stop	3244
diagnose sys scanunit dlp	3244
diagnose sys scanunit dlp config	3244
diagnose sys scanunit dlp config build	3245

diagnose sys scanunit dlp config status	3245
diagnose sys scanunit dlp config term	3245
diagnose sys scanunit dlp reset	3245
diagnose sys scanunit dlp status	3245
diagnose sys scanunit dlp threshold	3245
diagnose sys scanunit file-hash	3246
diagnose sys scanunit file-hash list	3246
diagnose sys scanunit file-hash list all	3246
diagnose sys scanunit file-hash list md5	3246
diagnose sys scanunit file-hash list sha1	3246
diagnose sys scanunit file-hash list sha256	3246
diagnose sys scanunit file-hash query	3247
diagnose sys scanunit file-hash query md5	3247
diagnose sys scanunit file-hash query sha1	3247
diagnose sys scanunit file-hash query sha256	3247
diagnose sys scanunit file-hash status	3247
diagnose sys scanunit filter	3248
diagnose sys scanunit filter clear	3248
diagnose sys scanunit filter list	3248
diagnose sys scanunit filter negate	3248
diagnose sys scanunit filter negate vd	3248
diagnose sys scanunit filter negate worker	3248
diagnose sys scanunit filter vd	3249
diagnose sys scanunit filter worker	3249
diagnose sys scanunit info	3249
diagnose sys scanunit info shared_status	3249
diagnose sys scanunit log	3249
diagnose sys scanunit log filter	3250
diagnose sys scanunit log filter clear	3250
diagnose sys scanunit log filter list	3250
diagnose sys scanunit log filter negate	3250
diagnose sys scanunit log filter negate vd	3250
diagnose sys scanunit log filter negate worker	3250
diagnose sys scanunit log filter vd	3251
diagnose sys scanunit log filter worker	3251
diagnose sys scanunit memory	3251
diagnose sys scanunit memory conserve	3251
diagnose sys scanunit memory conserve enter	3251
diagnose sys scanunit memory conserve exit	3252
diagnose sys scanunit restart	3252
diagnose sys scanunit simulate-crash	3252
diagnose sys scanunit simulate-crash lockup-workers	3252
diagnose sys scanunit simulate-crash lockup-workers all	3252
diagnose sys scanunit simulate-crash lockup-workers worker	3252
diagnose sys scanunit simulate-error	3253
diagnose sys scanunit simulate-error av-engine-delay	3253
diagnose sys scanunit simulate-error av-error	3253
diagnose sys scanunit simulate-error av-status	3253
diagnose sys scanunit simulate-error cdr-error	3254

diagnose sys scanunit simulate-error reset	3254
diagnose sys scanunit simulate-error scan-error-code	3254
diagnose sys scanunit simulate-error status	3254
diagnose sys scanunit stats	3254
diagnose sys scanunit stats all	3254
diagnose sys scanunit stats builder	3255
diagnose sys scanunit stats clear	3255
diagnose sys scanunit stats crash	3255
diagnose sys scanunit stats debug	3255
diagnose sys scanunit stats list	3255
diagnose sys scanunit stats manager	3255
diagnose sys scanunit stats worker	3256
diagnose sys scanunit valgrind	3256
diagnose sys scanunit valgrind disable	3256
diagnose sys scanunit valgrind enable	3256
diagnose sys scanunit valgrind log	3256
diagnose sys scanunit valgrind log clear	3256
diagnose sys scanunit valgrind log show	3257
diagnose sys scanunit valgrind memcheck	3257
diagnose sys scanunit valgrind memcheck_less	3257
diagnose sys scanunit valgrind status	3257
diagnose sys scanunit vdom-stats	3257
diagnose sys scanunit vdom-stats all	3257
diagnose sys scanunit vdom-stats clear	3258
diagnose sys scanunit vdom-stats clear-all	3258
diagnose sys scanunit vdom-stats list	3258
diagnose sys scanunit watchdog-override	3258
diagnose sys scanunit watchdog-override disable	3258
diagnose sys scanunit watchdog-override enable	3258
diagnose sys scanunit watchdog-override interval	3259
diagnose sys sccp-proxy	3259
diagnose sys sccp-proxy debug-console	3259
diagnose sys sccp-proxy phone	3259
diagnose sys sccp-proxy phone list	3259
diagnose sys sccp-proxy redirect	3259
diagnose sys sccp-proxy redirect list	3260
diagnose sys sccp-proxy restart	3260
diagnose sys sccp-proxy stats	3260
diagnose sys sccp-proxy stats clear	3260
diagnose sys sccp-proxy stats list	3260
diagnose sys sccp-proxy stats mem	3260
diagnose sys sccp-proxy stats mem full	3261
diagnose sys sccp-proxy stats mem summary	3261
diagnose sys sccp-proxy stats proto	3261
diagnose sys sccp-proxy valgrind	3261
diagnose sys sccp-proxy valgrind disable	3261
diagnose sys sccp-proxy valgrind enable	3261
diagnose sys sccp-proxy valgrind log	3262
diagnose sys sccp-proxy valgrind log clear	3262

diagnose sys sccp-proxy valgrind log show	3262
diagnose sys sccp-proxy valgrind memcheck	3262
diagnose sys sccp-proxy valgrind memcheck_less	3262
diagnose sys sccp-proxy valgrind status	3262
diagnose sys sdn	3263
diagnose sys sdn cache	3263
diagnose sys sdn status	3263
diagnose sys sdwan	3263
diagnose sys sdwan advpn	3264
diagnose sys sdwan advpn-session	3264
diagnose sys sdwan health-check	3264
diagnose sys sdwan health-check filter	3264
diagnose sys sdwan health-check filter clear	3264
diagnose sys sdwan health-check filter member	3264
diagnose sys sdwan health-check filter name	3265
diagnose sys sdwan health-check remote	3265
diagnose sys sdwan health-check status	3265
diagnose sys sdwan internet-service-app-ctrl-3t-set	3265
diagnose sys sdwan internet-service-app-ctrl-3t-unset	3266
diagnose sys sdwan internet-service-app-ctrl-flush	3266
diagnose sys sdwan internet-service-app-ctrl-list	3266
diagnose sys sdwan internet-service-app-ctrl-list app-id	3266
diagnose sys sdwan internet-service-app-ctrl-list cat-id	3267
diagnose sys sdwan internet-service-app-ctrl6-3t-set	3267
diagnose sys sdwan internet-service-app-ctrl6-3t-unset	3267
diagnose sys sdwan internet-service-app-ctrl6-flush	3268
diagnose sys sdwan internet-service-app-ctrl6-list	3268
diagnose sys sdwan internet-service-app-ctrl6-list app-id	3268
diagnose sys sdwan internet-service-app-ctrl6-list cat-id	3268
diagnose sys sdwan intf-sla-log	3268
diagnose sys sdwan log	3269
diagnose sys sdwan member	3269
diagnose sys sdwan neighbor	3269
diagnose sys sdwan reset	3269
diagnose sys sdwan route	3269
diagnose sys sdwan route6	3270
diagnose sys sdwan service4	3270
diagnose sys sdwan service6	3270
diagnose sys sdwan sla-log	3270
diagnose sys sdwan zone	3271
diagnose sys server-probe	3271
diagnose sys server-probe response	3271
diagnose sys service-communication	3271
diagnose sys session	3271
diagnose sys session clear	3272
diagnose sys session exp-stat	3272
diagnose sys session filter	3272
diagnose sys session filter clear	3272
diagnose sys session filter clear dintf	3272

diagnose sys session filter clear dport	3272
diagnose sys session filter clear dst	3273
diagnose sys session filter clear duration	3273
diagnose sys session filter clear expire	3273
diagnose sys session filter clear nport	3273
diagnose sys session filter clear nsrc	3273
diagnose sys session filter clear policy	3273
diagnose sys session filter clear proto	3274
diagnose sys session filter clear proto-state	3274
diagnose sys session filter clear session-state1	3274
diagnose sys session filter clear session-state2	3274
diagnose sys session filter clear sintf	3274
diagnose sys session filter clear sport	3274
diagnose sys session filter clear src	3275
diagnose sys session filter clear vd	3275
diagnose sys session filter dintf	3275
diagnose sys session filter dport	3275
diagnose sys session filter dst	3275
diagnose sys session filter duration	3276
diagnose sys session filter expire	3276
diagnose sys session filter ext-dst	3276
diagnose sys session filter ext-dst-negate	3276
diagnose sys session filter ext-src	3277
diagnose sys session filter ext-src-negate	3277
diagnose sys session filter negate	3277
diagnose sys session filter negate dintf	3277
diagnose sys session filter negate dport	3277
diagnose sys session filter negate dst	3278
diagnose sys session filter negate duration	3278
diagnose sys session filter negate expire	3278
diagnose sys session filter negate nport	3278
diagnose sys session filter negate nsrc	3278
diagnose sys session filter negate policy	3278
diagnose sys session filter negate proto	3279
diagnose sys session filter negate proto-state	3279
diagnose sys session filter negate session-state1	3279
diagnose sys session filter negate session-state2	3279
diagnose sys session filter negate sintf	3279
diagnose sys session filter negate sport	3279
diagnose sys session filter negate src	3280
diagnose sys session filter negate vd	3280
diagnose sys session filter nport	3280
diagnose sys session filter nsrc	3280
diagnose sys session filter policy	3280
diagnose sys session filter proto	3281
diagnose sys session filter proto-state	3281
diagnose sys session filter session-state1	3282
diagnose sys session filter session-state2	3282
diagnose sys session filter sintf	3282

diagnose sys session filter sport	3282
diagnose sys session filter src	3283
diagnose sys session filter vd	3283
diagnose sys session filter vd-name	3283
diagnose sys session full-stat	3283
diagnose sys session help	3283
diagnose sys session help add	3284
diagnose sys session help delete	3284
diagnose sys session help list	3284
diagnose sys session list	3284
diagnose sys session list expectation	3284
diagnose sys session stat	3285
diagnose sys session sync	3285
diagnose sys session sync reset	3285
diagnose sys session ttl	3285
diagnose sys session6	3285
diagnose sys session6 clear	3285
diagnose sys session6 exp-stat	3286
diagnose sys session6 filter	3286
diagnose sys session6 filter clear	3286
diagnose sys session6 filter clear dintf	3286
diagnose sys session6 filter clear dport	3286
diagnose sys session6 filter clear dst	3286
diagnose sys session6 filter clear duration	3287
diagnose sys session6 filter clear expire	3287
diagnose sys session6 filter clear nport	3287
diagnose sys session6 filter clear nsrc	3287
diagnose sys session6 filter clear policy	3287
diagnose sys session6 filter clear proto	3287
diagnose sys session6 filter clear proto-state	3288
diagnose sys session6 filter clear session-state1	3288
diagnose sys session6 filter clear session-state2	3288
diagnose sys session6 filter clear sintf	3288
diagnose sys session6 filter clear sport	3288
diagnose sys session6 filter clear src	3288
diagnose sys session6 filter clear vd	3289
diagnose sys session6 filter dintf	3289
diagnose sys session6 filter dport	3289
diagnose sys session6 filter dst	3289
diagnose sys session6 filter duration	3289
diagnose sys session6 filter expire	3290
diagnose sys session6 filter ext-dst	3290
diagnose sys session6 filter ext-dst-negate	3290
diagnose sys session6 filter ext-src	3290
diagnose sys session6 filter ext-src-negate	3291
diagnose sys session6 filter negate	3291
diagnose sys session6 filter negate dintf	3291
diagnose sys session6 filter negate dport	3291
diagnose sys session6 filter negate dst	3291

diagnose sys session6 filter negate duration	3292
diagnose sys session6 filter negate expire	3292
diagnose sys session6 filter negate nport	3292
diagnose sys session6 filter negate nsrc	3292
diagnose sys session6 filter negate policy	3292
diagnose sys session6 filter negate proto	3292
diagnose sys session6 filter negate proto-state	3293
diagnose sys session6 filter negate session-state1	3293
diagnose sys session6 filter negate session-state2	3293
diagnose sys session6 filter negate sintf	3293
diagnose sys session6 filter negate sport	3293
diagnose sys session6 filter negate src	3293
diagnose sys session6 filter negate vd	3294
diagnose sys session6 filter nport	3294
diagnose sys session6 filter nsrc	3294
diagnose sys session6 filter policy	3294
diagnose sys session6 filter proto	3295
diagnose sys session6 filter proto-state	3295
diagnose sys session6 filter session-state1	3295
diagnose sys session6 filter session-state2	3295
diagnose sys session6 filter sintf	3296
diagnose sys session6 filter sport	3296
diagnose sys session6 filter src	3296
diagnose sys session6 filter vd	3296
diagnose sys session6 filter vd-name	3297
diagnose sys session6 full-stat	3297
diagnose sys session6 help	3297
diagnose sys session6 help add	3297
diagnose sys session6 help delete	3298
diagnose sys session6 help list	3298
diagnose sys session6 list	3298
diagnose sys session6 list expectation	3298
diagnose sys session6 stat	3298
diagnose sys session6 sync	3298
diagnose sys session6 sync reset	3299
diagnose sys shmfile	3299
diagnose sys shmfile dump	3299
diagnose sys shmfile dump oid-app	3299
diagnose sys shmfile dump oid-slab	3299
diagnose sys shmfile dump slab-file	3300
diagnose sys shmfile dump table-count	3300
diagnose sys shmfile dump table-count total	3300
diagnose sys shmfile dump table-count vdom	3300
diagnose sys shmfile dump vdom	3300
diagnose sys sip	3301
diagnose sys sip debug-mask	3301
diagnose sys sip dialog	3301
diagnose sys sip dialog clear	3301
diagnose sys sip dialog list	3301

diagnose sys sip mapping	3302
diagnose sys sip mapping list	3302
diagnose sys sip status	3302
diagnose sys sip-proxy	3302
diagnose sys sip-proxy alg	3302
diagnose sys sip-proxy alg bypass	3302
diagnose sys sip-proxy alg parse-only	3303
diagnose sys sip-proxy calls	3303
diagnose sys sip-proxy calls clear	3303
diagnose sys sip-proxy calls idle	3303
diagnose sys sip-proxy calls invite	3303
diagnose sys sip-proxy calls list	3303
diagnose sys sip-proxy config	3304
diagnose sys sip-proxy config list	3304
diagnose sys sip-proxy config profiles	3304
diagnose sys sip-proxy debug-console	3304
diagnose sys sip-proxy filter	3304
diagnose sys sip-proxy filter clear	3304
diagnose sys sip-proxy filter dst-addr4	3305
diagnose sys sip-proxy filter dst-addr6	3305
diagnose sys sip-proxy filter dst-port	3305
diagnose sys sip-proxy filter list	3305
diagnose sys sip-proxy filter negate	3306
diagnose sys sip-proxy filter negate dst-addr4	3306
diagnose sys sip-proxy filter negate dst-addr6	3306
diagnose sys sip-proxy filter negate dst-port	3306
diagnose sys sip-proxy filter negate policy	3306
diagnose sys sip-proxy filter negate policy-type	3306
diagnose sys sip-proxy filter negate src-addr4	3307
diagnose sys sip-proxy filter negate src-addr6	3307
diagnose sys sip-proxy filter negate src-port	3307
diagnose sys sip-proxy filter negate vd	3307
diagnose sys sip-proxy filter negate voip-profile	3307
diagnose sys sip-proxy filter policy	3307
diagnose sys sip-proxy filter policy-type	3308
diagnose sys sip-proxy filter policy-type ipv4	3308
diagnose sys sip-proxy filter policy-type ipv6	3308
diagnose sys sip-proxy filter src-addr4	3308
diagnose sys sip-proxy filter src-addr6	3308
diagnose sys sip-proxy filter src-port	3309
diagnose sys sip-proxy filter vd	3309
diagnose sys sip-proxy filter voip-profile	3309
diagnose sys sip-proxy log-filter	3309
diagnose sys sip-proxy log-filter clear	3310
diagnose sys sip-proxy log-filter dst-addr4	3310
diagnose sys sip-proxy log-filter dst-addr6	3310
diagnose sys sip-proxy log-filter dst-port	3310
diagnose sys sip-proxy log-filter list	3311
diagnose sys sip-proxy log-filter negate	3311

diagnose sys sip-proxy log-filter negate dst-addr4	3311
diagnose sys sip-proxy log-filter negate dst-addr6	3311
diagnose sys sip-proxy log-filter negate dst-port	3311
diagnose sys sip-proxy log-filter negate policy	3311
diagnose sys sip-proxy log-filter negate policy-type	3312
diagnose sys sip-proxy log-filter negate src-addr4	3312
diagnose sys sip-proxy log-filter negate src-addr6	3312
diagnose sys sip-proxy log-filter negate src-port	3312
diagnose sys sip-proxy log-filter negate vd	3312
diagnose sys sip-proxy log-filter negate voip-profile	3312
diagnose sys sip-proxy log-filter policy	3313
diagnose sys sip-proxy log-filter policy-type	3313
diagnose sys sip-proxy log-filter policy-type ipv4	3313
diagnose sys sip-proxy log-filter policy-type ipv6	3313
diagnose sys sip-proxy log-filter src-addr4	3313
diagnose sys sip-proxy log-filter src-addr6	3314
diagnose sys sip-proxy log-filter src-port	3314
diagnose sys sip-proxy log-filter vd	3314
diagnose sys sip-proxy log-filter voip-profile	3314
diagnose sys sip-proxy meters	3315
diagnose sys sip-proxy meters list	3315
diagnose sys sip-proxy redirect	3315
diagnose sys sip-proxy redirect list	3315
diagnose sys sip-proxy restart	3315
diagnose sys sip-proxy scheduler-times	3315
diagnose sys sip-proxy scheduler-times display	3316
diagnose sys sip-proxy scheduler-times start	3316
diagnose sys sip-proxy scheduler-times stop	3316
diagnose sys sip-proxy session	3316
diagnose sys sip-proxy session list	3316
diagnose sys sip-proxy ssl	3316
diagnose sys sip-proxy ssl hardware	3317
diagnose sys sip-proxy ssl software	3317
diagnose sys sip-proxy stats	3317
diagnose sys sip-proxy stats call	3317
diagnose sys sip-proxy stats clear	3317
diagnose sys sip-proxy stats ha	3317
diagnose sys sip-proxy stats list	3318
diagnose sys sip-proxy stats mem	3318
diagnose sys sip-proxy stats mem full	3318
diagnose sys sip-proxy stats mem summary	3318
diagnose sys sip-proxy stats proto	3318
diagnose sys sip-proxy stats ssl-auth	3318
diagnose sys sip-proxy stats udp	3319
diagnose sys sip-proxy valgrind	3319
diagnose sys sip-proxy valgrind disable	3319
diagnose sys sip-proxy valgrind enable	3319
diagnose sys sip-proxy valgrind log	3319
diagnose sys sip-proxy valgrind log clear	3319

diagnose sys sip-proxy valgrind log show	3320
diagnose sys sip-proxy valgrind memcheck	3320
diagnose sys sip-proxy valgrind memcheck_less	3320
diagnose sys sip-proxy valgrind status	3320
diagnose sys sip-proxy vdom	3320
diagnose sys sip-proxy vdom list	3320
diagnose sys sip-proxy vip	3321
diagnose sys sip-proxy vip real-server	3321
diagnose sys speedtest-server	3321
diagnose sys speedtest-server clients	3321
diagnose sys speedtest-server clients flush	3321
diagnose sys speedtest-server clients list	3321
diagnose sys speedtest-server controller	3322
diagnose sys speedtest-server controller add	3322
diagnose sys speedtest-server controller del	3322
diagnose sys speedtest-server controller list	3322
diagnose sys speedtest-server log	3322
diagnose sys speedtest-server log del-file	3323
diagnose sys speedtest-server log list	3323
diagnose sys speedtest-server log load-disk	3323
diagnose sys speedtest-server log save-disk	3323
diagnose sys speedtest-server speedtest-dbg	3323
diagnose sys tcp-auth-options	3323
diagnose sys tcp-option	3324
diagnose sys tcp-option dump	3324
diagnose sys tcp-option sack	3324
diagnose sys tcp-option sack disable	3324
diagnose sys tcp-option sack enable	3324
diagnose sys tcp-option timestamps	3324
diagnose sys tcp-option timestamps disable	3325
diagnose sys tcp-option timestamps enable	3325
diagnose sys tcp-option window-scale	3325
diagnose sys tcp-option window-scale disable	3325
diagnose sys tcp-option window-scale enable	3325
diagnose sys tcpsock	3325
diagnose sys tcpsock6	3326
diagnose sys top	3326
diagnose sys top-all	3326
diagnose sys top-fd	3326
diagnose sys top-fd detail	3327
diagnose sys top-mem	3327
diagnose sys top-mem detail	3327
diagnose sys top-sockmem	3327
diagnose sys traffic	3328
diagnose sys traffic app-stats	3328
diagnose sys traffic app-stats add	3328
diagnose sys traffic app-stats del	3328
diagnose sys traffic app-stats hash-stats	3328
diagnose sys traffic app-stats list	3329

diagnose sys traffic statistics	3329
diagnose sys traffic statistics clear	3329
diagnose sys traffic statistics show	3329
diagnose sys traffic-priority	3329
diagnose sys traffic-priority list	3329
diagnose sys udp-reserved-port	3330
diagnose sys udp-reserved-port test	3330
diagnose sys udpsock	3330
diagnose sys udpsock6	3330
diagnose sys upgrade-report	3330
diagnose sys upgrade-report current	3330
diagnose sys upgrade-report generate	3331
diagnose sys upgrade-report on-disk	3331
diagnose sys uuid	3331
diagnose sys uuid allow-manual-set	3331
diagnose sys uuid allow-manual-set disable	3331
diagnose sys uuid allow-manual-set enable	3331
diagnose sys uuid generate	3332
diagnose sys var-zone	3332
diagnose sys var-zone show	3332
diagnose sys vd	3332
diagnose sys vd add	3332
diagnose sys vd delete	3332
diagnose sys vd list	3333
diagnose sys vd set	3333
diagnose sys vd stats	3333
diagnose sys vdom-property	3333
diagnose sys vlan	3333
diagnose sys vlan list	3334
diagnose sys vxlan	3334
diagnose sys vxlan device	3334
diagnose sys vxlan device list	3334
diagnose sys vxlan fdb	3334
diagnose sys vxlan fdb list	3334
diagnose sys vxlan fdb stat	3335
diagnose sys waninfo	3335
diagnose sys waninfo ipify	3335
diagnose sys wccp	3335
diagnose sys wccp delete	3335
diagnose sys wccp flush	3336
diagnose sys wccp list	3336
diagnose test analytics-pdf-report	3336
diagnose test analytics-pdf-report list	3336
diagnose test analytics-pdf-report max	3336
diagnose test analytics-pdf-report request	3337
diagnose test analytics-pdf-report status	3337
diagnose test analytics-report	3337
diagnose test analytics-report checksum	3337
diagnose test application	3337

diagnose test application acd	3339
diagnose test application acsd	3340
diagnose test application autod	3340
diagnose test application awsd	3340
diagnose test application azd	3340
diagnose test application bfd	3340
diagnose test application cloudapid	3341
diagnose test application cmdbsvr	3341
diagnose test application csfd	3341
diagnose test application ddnsd	3341
diagnose test application dhcp6c	3342
diagnose test application dhcp6r	3342
diagnose test application dhcprelay	3342
diagnose test application dlpfingerprint	3342
diagnose test application dlpfpcache	3343
diagnose test application dnsproxy	3343
diagnose test application dsd	3343
diagnose test application eap_supp	3343
diagnose test application evpn	3344
diagnose test application fas	3344
diagnose test application fcnacd	3344
diagnose test application fds_notify	3344
diagnose test application fgtlogd	3344
diagnose test application fnbamd	3345
diagnose test application forticldd	3345
diagnose test application forticron	3345
diagnose test application fortimq	3345
diagnose test application fsvrd	3346
diagnose test application gcpd	3346
diagnose test application harelay	3346
diagnose test application hasync	3346
diagnose test application hatalk	3347
diagnose test application ibmd	3347
diagnose test application imap	3347
diagnose test application init	3347
diagnose test application iotd	3347
diagnose test application ipamd	3348
diagnose test application ipamsd	3348
diagnose test application ipldbd	3348
diagnose test application ipsengine	3348
diagnose test application ipsmonitor	3349
diagnose test application ipsufd	3349
diagnose test application kmipd	3349
diagnose test application kubed	3349
diagnose test application l2tpcd	3350
diagnose test application lnkmt	3350
diagnose test application locallogd	3350
diagnose test application miglogd	3350
diagnose test application mrd	3351

diagnose test application netxd	3351
diagnose test application nntp	3351
diagnose test application ocid	3351
diagnose test application openstackd	3352
diagnose test application ovrd	3352
diagnose test application pcpd	3352
diagnose test application pop3	3352
diagnose test application pptpcd	3353
diagnose test application quarantined	3353
diagnose test application radius-das	3353
diagnose test application radiusd	3353
diagnose test application radvd	3354
diagnose test application reportd	3354
diagnose test application sdncd	3354
diagnose test application sdnd	3354
diagnose test application sepmd	3354
diagnose test application sessionsync	3355
diagnose test application sflowd	3355
diagnose test application sfupgraded	3355
diagnose test application smtp	3355
diagnose test application snmpd	3356
diagnose test application syslogd	3356
diagnose test application updated	3356
diagnose test application uploadd	3356
diagnose test application urlfilter	3357
diagnose test application vned	3357
diagnose test application vrrp	3357
diagnose test application waagent	3357
diagnose test application wad	3358
diagnose test application wccpd	3358
diagnose test application wf_monitor	3358
diagnose test application wiredapd	3358
diagnose test application zebos_launcher	3359
diagnose test authserver	3359
diagnose test authserver cert	3359
diagnose test authserver ext-idp	3359
diagnose test authserver ldap	3360
diagnose test authserver ldap-digest	3360
diagnose test authserver ldap-direct	3360
diagnose test authserver ldap-search	3360
diagnose test authserver local	3360
diagnose test authserver pop3	3360
diagnose test authserver radius	3361
diagnose test authserver radius-direct	3361
diagnose test authserver tacacs+	3361
diagnose test authserver tacacs+-direct	3361
diagnose test authserver user	3361
diagnose test guest	3362
diagnose test guest add	3362

diagnose test guest del	3362
diagnose test guest list	3362
diagnose test scim	3362
diagnose test scim get-group	3363
diagnose test scim get-membership	3363
diagnose test scim get-user	3363
diagnose test scim list-clients	3363
diagnose test scim list-groups	3363
diagnose test scim list-users	3363
diagnose test security	3364
diagnose test security mount-invalid-flag	3364
diagnose test security status	3364
diagnose test update	3364
diagnose test update info	3364
diagnose test update tzdb	3364
diagnose traffictest	3365
diagnose traffictest client-intf	3365
diagnose traffictest port	3365
diagnose traffictest proto	3365
diagnose traffictest proto 0	3366
diagnose traffictest proto 1	3366
diagnose traffictest run	3366
diagnose traffictest server-intf	3367
diagnose traffictest show	3367
diagnose user	3367
diagnose user banned-ip	3368
diagnose user banned-ip add	3368
diagnose user banned-ip add src4	3368
diagnose user banned-ip add src6	3369
diagnose user banned-ip clear	3369
diagnose user banned-ip delete	3369
diagnose user banned-ip delete src4	3369
diagnose user banned-ip delete src6	3369
diagnose user banned-ip list	3370
diagnose user banned-ip list all	3370
diagnose user banned-ip list src4	3370
diagnose user banned-ip list src6	3370
diagnose user banned-ip stat	3370
diagnose user banned-ip stress-test	3370
diagnose user device	3371
diagnose user device clear	3371
diagnose user device clear vd	3371
diagnose user device del	3371
diagnose user device get	3372
diagnose user device list	3372
diagnose user device list vd	3372
diagnose user device stats	3372
diagnose user-device-store	3372

diagnose user-device-store device	3374
diagnose user-device-store device disk	3375
diagnose user-device-store device disk clear	3375
diagnose user-device-store device disk list	3375
diagnose user-device-store device disk query	3375
diagnose user-device-store device fortifone	3375
diagnose user-device-store device fortifone add	3375
diagnose user-device-store device fortifone delete	3376
diagnose user-device-store device fortifone list	3376
diagnose user-device-store device memory	3376
diagnose user-device-store device memory list	3376
diagnose user-device-store device memory mac-host	3376
diagnose user-device-store device memory mac-host add	3376
diagnose user-device-store device memory mac-host query	3377
diagnose user-device-store device memory mac-host subscribe	3377
diagnose user-device-store device memory mac-host subscribe disable	3377
diagnose user-device-store device memory mac-host subscribe enable	3377
diagnose user-device-store device memory mac-host validate	3377
diagnose user-device-store device memory ot-purdue-set	3378
diagnose user-device-store device memory query	3378
diagnose user-device-store device memory uid	3378
diagnose user-device-store device memory uid add	3378
diagnose user-device-store device memory uid delete	3378
diagnose user-device-store device memory uid update	3378
diagnose user-device-store device memory vulnerability-clear	3379
diagnose user-device-store device memory vulnerability-clear-all	3379
diagnose user-device-store device memory vulnerability-detected	3379
diagnose user-device-store device memory vulnerability-query	3379
diagnose user-device-store device memory vulnerability-update	3379
diagnose user-device-store device-stats-query	3380
diagnose user-device-store device-stats-query filters-and	3380
diagnose user-device-store device-stats-query filters-or	3380
diagnose user-device-store email-stats	3380
diagnose user-device-store email-stats list	3380
diagnose user-device-store email-stats query	3380
diagnose user-device-store fsw-device-stats-query	3381
diagnose user-device-store fsw-device-stats-query filters-and	3381
diagnose user-device-store fsw-device-stats-query filters-or	3381
diagnose user-device-store ftcl-device-stats-query	3381
diagnose user-device-store ftcl-device-stats-query filters-and	3381
diagnose user-device-store ftcl-device-stats-query filters-or	3382
diagnose user-device-store iot-ot-vuln	3382
diagnose user-device-store iot-ot-vuln list	3382
diagnose user-device-store iot-ot-vuln query	3382
diagnose user-device-store unified	3382
diagnose user-device-store unified clear	3382
diagnose user-device-store unified debug	3383
diagnose user-device-store unified debug disable	3383
diagnose user-device-store unified debug enable	3383

diagnose user-device-store unified delete	3383
diagnose user-device-store unified device-memory-query	3383
diagnose user-device-store unified device-memory-query filters-and	3383
diagnose user-device-store unified device-memory-query filters-or	3384
diagnose user-device-store unified device-query	3384
diagnose user-device-store unified device-query filters-and	3384
diagnose user-device-store unified device-query filters-or	3384
diagnose user-device-store unified dump	3384
diagnose user-device-store unified list	3384
diagnose user-device-store unified re-query	3385
diagnose user-device-store unified stats	3385
diagnose user-device-store unified user-memory-query	3385
diagnose user-device-store unified user-memory-query filters-and	3385
diagnose user-device-store unified user-memory-query filters-or	3385
diagnose user-device-store unified user-query	3385
diagnose user-device-store unified user-query filters-and	3386
diagnose user-device-store unified user-query filters-or	3386
diagnose user-device-store user	3386
diagnose user-device-store user disk	3386
diagnose user-device-store user disk clear	3386
diagnose user-device-store user disk list	3386
diagnose user-device-store user disk query	3387
diagnose user-device-store user memory	3387
diagnose user-device-store user memory list	3387
diagnose user-device-store user memory query	3387
diagnose user-device-store user-count	3387
diagnose user-device-store user-count list	3387
diagnose user-device-store user-count query	3388
diagnose user-device-store user-stats	3388
diagnose user-device-store user-stats query	3388
diagnose vendor-mac	3388
diagnose vendor-mac id	3388
diagnose vendor-mac id-summary	3389
diagnose vendor-mac info	3389
diagnose vendor-mac match	3389
diagnose vpn ike	3389
diagnose vpn ike admin	3392
diagnose vpn ike config	3392
diagnose vpn ike config list	3392
diagnose vpn ike config list summary	3392
diagnose vpn ike counts	3392
diagnose vpn ike crash	3392
diagnose vpn ike crypto	3393
diagnose vpn ike crypto stats	3393
diagnose vpn ike errors	3393
diagnose vpn ike fragmentation-override	3393
diagnose vpn ike gateway	3393
diagnose vpn ike gateway clear	3393
diagnose vpn ike gateway clear name	3394

diagnose vpn ike gateway filter	3394
diagnose vpn ike gateway filter clear	3394
diagnose vpn ike gateway filter dst-port	3394
diagnose vpn ike gateway filter ifindex	3394
diagnose vpn ike gateway filter loc-addr4	3395
diagnose vpn ike gateway filter loc-addr6	3395
diagnose vpn ike gateway filter name	3395
diagnose vpn ike gateway filter negate	3395
diagnose vpn ike gateway filter negate dst-port	3396
diagnose vpn ike gateway filter negate ifindex	3396
diagnose vpn ike gateway filter negate loc-addr4	3396
diagnose vpn ike gateway filter negate loc-addr6	3396
diagnose vpn ike gateway filter negate name	3396
diagnose vpn ike gateway filter negate rem-addr4	3396
diagnose vpn ike gateway filter negate rem-addr6	3397
diagnose vpn ike gateway filter negate vd	3397
diagnose vpn ike gateway filter rem-addr4	3397
diagnose vpn ike gateway filter rem-addr6	3397
diagnose vpn ike gateway filter vd	3397
diagnose vpn ike gateway flush	3398
diagnose vpn ike gateway flush name	3398
diagnose vpn ike gateway list	3398
diagnose vpn ike gateway list name	3398
diagnose vpn ike ikev2-cookie-enforce	3398
diagnose vpn ike log	3399
diagnose vpn ike log filter	3399
diagnose vpn ike log filter clear	3399
diagnose vpn ike log filter dst-port	3399
diagnose vpn ike log filter ifindex	3399
diagnose vpn ike log filter list	3400
diagnose vpn ike log filter loc-addr4	3400
diagnose vpn ike log filter loc-addr6	3400
diagnose vpn ike log filter mloc-addr4	3400
diagnose vpn ike log filter mloc-addr6	3401
diagnose vpn ike log filter mrem-addr4	3401
diagnose vpn ike log filter mrem-addr6	3402
diagnose vpn ike log filter name	3403
diagnose vpn ike log filter negate	3403
diagnose vpn ike log filter negate dst-port	3403
diagnose vpn ike log filter negate ifindex	3403
diagnose vpn ike log filter negate loc-addr4	3403
diagnose vpn ike log filter negate loc-addr6	3403
diagnose vpn ike log filter negate mloc-addr4	3404
diagnose vpn ike log filter negate mloc-addr6	3404
diagnose vpn ike log filter negate mrem-addr4	3404
diagnose vpn ike log filter negate mrem-addr6	3404
diagnose vpn ike log filter negate name	3404
diagnose vpn ike log filter negate rem-addr4	3404
diagnose vpn ike log filter negate rem-addr6	3405

diagnose vpn ike log filter negate vd	3405
diagnose vpn ike log filter rem-addr4	3405
diagnose vpn ike log filter rem-addr6	3405
diagnose vpn ike log filter vd	3405
diagnose vpn ike log function-name	3406
diagnose vpn ike log function-name disable	3406
diagnose vpn ike log function-name enable	3406
diagnose vpn ike log terminal	3406
diagnose vpn ike log terminal clear	3406
diagnose vpn ike log terminal reset	3406
diagnose vpn ike log terminal stats	3407
diagnose vpn ike manager	3407
diagnose vpn ike qkd	3407
diagnose vpn ike restart	3407
diagnose vpn ike routes	3407
diagnose vpn ike routes list	3407
diagnose vpn ike secrets	3408
diagnose vpn ike stats	3408
diagnose vpn ike status	3408
diagnose vpn ike status detailed	3408
diagnose vpn ike status summary	3408
diagnose vpn ike valgrind	3408
diagnose vpn ike valgrind disable	3409
diagnose vpn ike valgrind enable	3409
diagnose vpn ike valgrind log	3409
diagnose vpn ike valgrind log clear	3409
diagnose vpn ike valgrind log show	3409
diagnose vpn ike valgrind memcheck	3409
diagnose vpn ike valgrind memcheck_less	3410
diagnose vpn ike valgrind status	3410
diagnose vpn ikecrypt	3410
diagnose vpn ikecrypt info	3410
diagnose vpn ikecrypt restart	3410
diagnose vpn ikecrypt valgrind	3411
diagnose vpn ikecrypt valgrind disable	3411
diagnose vpn ikecrypt valgrind enable	3411
diagnose vpn ikecrypt valgrind log	3411
diagnose vpn ikecrypt valgrind log clear	3411
diagnose vpn ikecrypt valgrind log show	3411
diagnose vpn ikecrypt valgrind memcheck	3412
diagnose vpn ikecrypt valgrind memcheck_less	3412
diagnose vpn ikecrypt valgrind status	3412
diagnose vpn ipsec	3412
diagnose vpn ipsec cpu	3412
diagnose vpn ipsec cpu clear	3412
diagnose vpn ipsec status	3413
diagnose vpn l2tp	3413
diagnose vpn l2tp status	3413
diagnose vpn l2tp tunnel	3413

diagnose vpn mr	3413
diagnose vpn mr add	3414
diagnose vpn mr del	3414
diagnose vpn mr list-addr	3414
diagnose vpn mr list-dev	3415
diagnose vpn mr list-tun	3415
diagnose vpn mr6	3415
diagnose vpn mr6 add	3415
diagnose vpn mr6 del	3416
diagnose vpn mr6 list-addr	3416
diagnose vpn mr6 list-dev	3416
diagnose vpn mr6 list-tun	3417
diagnose vpn pptp	3417
diagnose vpn pptp status	3417
diagnose vpn ssl	3417
diagnose vpn ssl app-session	3418
diagnose vpn ssl blocklist	3418
diagnose vpn ssl blocklist count	3419
diagnose vpn ssl blocklist del	3419
diagnose vpn ssl blocklist list	3419
diagnose vpn ssl cmdb-cache-log	3419
diagnose vpn ssl debug-filter	3420
diagnose vpn ssl debug-filter clear	3420
diagnose vpn ssl debug-filter list	3420
diagnose vpn ssl debug-filter negate	3420
diagnose vpn ssl debug-filter negate src-addr4	3420
diagnose vpn ssl debug-filter negate src-addr6	3420
diagnose vpn ssl debug-filter negate vd	3421
diagnose vpn ssl debug-filter src-addr4	3421
diagnose vpn ssl debug-filter src-addr6	3421
diagnose vpn ssl debug-filter vd	3421
diagnose vpn ssl dist-usr	3422
diagnose vpn ssl dist-usr count	3422
diagnose vpn ssl dist-usr del	3422
diagnose vpn ssl dist-usr list	3422
diagnose vpn ssl info	3423
diagnose vpn ssl list	3423
diagnose vpn ssl peer-name	3423
diagnose vpn ssl peer-name count	3423
diagnose vpn ssl peer-name del	3423
diagnose vpn ssl peer-name list	3424
diagnose vpn ssl saml-metadata	3424
diagnose vpn ssl statistics	3424
diagnose vpn ssl user-session	3424
diagnose vpn ssl usr-chg	3425
diagnose vpn ssl usr-chg count	3425
diagnose vpn ssl usr-chg del	3425
diagnose vpn ssl usr-chg list	3425
diagnose vpn ssl web-mode-test	3426

diagnose vpn tunnel	3426
diagnose vpn tunnel bundle-list	3426
diagnose vpn tunnel bundle-list name	3427
diagnose vpn tunnel bundle-list vdom	3427
diagnose vpn tunnel delinbsa	3427
diagnose vpn tunnel deloutbsa	3427
diagnose vpn tunnel dialup-list	3428
diagnose vpn tunnel down	3428
diagnose vpn tunnel fec	3428
diagnose vpn tunnel flush	3429
diagnose vpn tunnel key-life-time	3429
diagnose vpn tunnel list	3429
diagnose vpn tunnel list name	3429
diagnose vpn tunnel list number	3429
diagnose vpn tunnel route4-priority	3430
diagnose vpn tunnel route6-priority	3430
diagnose vpn tunnel stat	3430
diagnose vpn tunnel stat flush	3430
diagnose vpn tunnel up	3430
diagnose wacs	3431
diagnose wacs clear	3431
diagnose wacs restart	3431
diagnose wacs stats	3431
diagnose wad	3431
diagnose wad access-proxy	3443
diagnose wad access-proxy health-check	3443
diagnose wad access-proxy health-check status	3443
diagnose wad config	3443
diagnose wad config auth-rule	3443
diagnose wad config policy	3443
diagnose wad config proxy-policy	3444
diagnose wad config summary	3444
diagnose wad console-log	3444
diagnose wad console-log disable	3444
diagnose wad console-log enable	3444
diagnose wad csvc	3444
diagnose wad csvc bytecache	3445
diagnose wad csvc bytecache clear	3445
diagnose wad csvc bytecache flush	3445
diagnose wad csvc bytecache lists	3445
diagnose wad csvc bytecache stats	3445
diagnose wad csvc bytecache toggle	3446
diagnose wad csvc bytecache toggle all	3446
diagnose wad csvc bytecache toggle create	3446
diagnose wad csvc bytecache toggle read	3446
diagnose wad csvc memcache	3447
diagnose wad csvc memcache clear	3447
diagnose wad csvc memcache flush	3447
diagnose wad csvc memcache lists	3447

diagnose wad csvc memcache stats	3447
diagnose wad csvc restart	3448
diagnose wad csvc webcache	3448
diagnose wad csvc webcache clear	3448
diagnose wad csvc webcache flush	3448
diagnose wad csvc webcache lists	3449
diagnose wad csvc webcache stats	3449
diagnose wad csvc webcache toggle	3449
diagnose wad csvc webcache toggle abort	3449
diagnose wad csvc webcache toggle add_ref	3449
diagnose wad csvc webcache toggle all	3450
diagnose wad csvc webcache toggle append	3450
diagnose wad csvc webcache toggle create	3450
diagnose wad csvc webcache toggle read	3450
diagnose wad csvc webcache toggle remove	3451
diagnose wad csvc webcache toggle resolve	3451
diagnose wad csvc webcache toggle update	3451
diagnose wad debug	3451
diagnose wad debug clear	3451
diagnose wad debug crash	3452
diagnose wad debug crash clear	3452
diagnose wad debug crash disable	3452
diagnose wad debug crash enable	3452
diagnose wad debug crash list	3452
diagnose wad debug crash max	3452
diagnose wad debug crash read	3453
diagnose wad debug disable	3453
diagnose wad debug disable category	3453
diagnose wad debug disable category antiphish	3453
diagnose wad debug disable category auth	3453
diagnose wad debug disable category autotest	3453
diagnose wad debug disable category bytcache	3454
diagnose wad debug disable category casb	3454
diagnose wad debug disable category cifs	3454
diagnose wad debug disable category cmgr	3454
diagnose wad debug disable category config	3454
diagnose wad debug disable category csvc	3454
diagnose wad debug disable category detail	3455
diagnose wad debug disable category devuln	3455
diagnose wad debug disable category diag	3455
diagnose wad debug disable category dispatcher	3455
diagnose wad debug disable category dns	3455
diagnose wad debug disable category dskd	3455
diagnose wad debug disable category email	3456
diagnose wad debug disable category ftp	3456
diagnose wad debug disable category http	3456
diagnose wad debug disable category http2	3456
diagnose wad debug disable category http3	3456
diagnose wad debug disable category icap	3456

diagnose wad debug disable category icbsvc	3457
diagnose wad debug disable category info	3457
diagnose wad debug disable category ips	3457
diagnose wad debug disable category mapi	3457
diagnose wad debug disable category memblk	3457
diagnose wad debug disable category monitor	3457
diagnose wad debug disable category packet	3458
diagnose wad debug disable category policy	3458
diagnose wad debug disable category policy_test	3458
diagnose wad debug disable category proc	3458
diagnose wad debug disable category quic	3458
diagnose wad debug disable category quic_cc	3458
diagnose wad debug disable category rpc	3459
diagnose wad debug disable category scan	3459
diagnose wad debug disable category scp	3459
diagnose wad debug disable category session	3459
diagnose wad debug disable category sftp	3459
diagnose wad debug disable category socks	3459
diagnose wad debug disable category ssh	3460
diagnose wad debug disable category ssl	3460
diagnose wad debug disable category stream	3460
diagnose wad debug disable category svc_conn	3460
diagnose wad debug disable category sys	3460
diagnose wad debug disable category tfap	3460
diagnose wad debug disable category tls_fingerprint	3461
diagnose wad debug disable category tunnel	3461
diagnose wad debug disable category uih	3461
diagnose wad debug disable category video	3461
diagnose wad debug disable category vs	3461
diagnose wad debug disable category webcache	3461
diagnose wad debug disable category ztna_portal	3462
diagnose wad debug disable category ztna_rev_conn	3462
diagnose wad debug display	3462
diagnose wad debug display pid	3462
diagnose wad debug display pid disable	3462
diagnose wad debug display pid enable	3462
diagnose wad debug enable	3463
diagnose wad debug enable all	3463
diagnose wad debug enable category	3463
diagnose wad debug enable category all	3463
diagnose wad debug enable category antiphish	3463
diagnose wad debug enable category auth	3463
diagnose wad debug enable category autotest	3464
diagnose wad debug enable category bytecache	3464
diagnose wad debug enable category casb	3464
diagnose wad debug enable category cifs	3464
diagnose wad debug enable category cmgr	3464
diagnose wad debug enable category config	3464
diagnose wad debug enable category csvc	3465

diagnose wad debug enable category detail	3465
diagnose wad debug enable category devuln	3465
diagnose wad debug enable category diag	3465
diagnose wad debug enable category dispatcher	3465
diagnose wad debug enable category dns	3465
diagnose wad debug enable category dskd	3466
diagnose wad debug enable category email	3466
diagnose wad debug enable category ftp	3466
diagnose wad debug enable category http	3466
diagnose wad debug enable category http2	3466
diagnose wad debug enable category http3	3466
diagnose wad debug enable category icap	3467
diagnose wad debug enable category icbsvc	3467
diagnose wad debug enable category info	3467
diagnose wad debug enable category ips	3467
diagnose wad debug enable category mapi	3467
diagnose wad debug enable category memblk	3467
diagnose wad debug enable category monitor	3468
diagnose wad debug enable category packet	3468
diagnose wad debug enable category policy	3468
diagnose wad debug enable category policy_test	3468
diagnose wad debug enable category proc	3468
diagnose wad debug enable category quic	3468
diagnose wad debug enable category quic_cc	3469
diagnose wad debug enable category rpc	3469
diagnose wad debug enable category scan	3469
diagnose wad debug enable category scp	3469
diagnose wad debug enable category session	3469
diagnose wad debug enable category sftp	3469
diagnose wad debug enable category socks	3470
diagnose wad debug enable category ssh	3470
diagnose wad debug enable category ssl	3470
diagnose wad debug enable category stream	3470
diagnose wad debug enable category svc_conn	3470
diagnose wad debug enable category sys	3470
diagnose wad debug enable category tfap	3471
diagnose wad debug enable category tls_fingerprint	3471
diagnose wad debug enable category tunnel	3471
diagnose wad debug enable category uih	3471
diagnose wad debug enable category video	3471
diagnose wad debug enable category vs	3471
diagnose wad debug enable category webcache	3472
diagnose wad debug enable category ztna_portal	3472
diagnose wad debug enable category ztna_rev_conn	3472
diagnose wad debug enable level	3472
diagnose wad debug enable level error	3472
diagnose wad debug enable level info	3472
diagnose wad debug enable level verbose	3473
diagnose wad debug enable level warn	3473

diagnose wad debug ips-db	3473
diagnose wad debug ips-db status	3473
diagnose wad debug ips-filter	3473
diagnose wad debug ips-filter aid	3473
diagnose wad debug ips-filter all	3474
diagnose wad debug ips-filter clear	3474
diagnose wad debug ips-filter show	3474
diagnose wad debug ips-filter vid	3474
diagnose wad debug save-http-req-crash	3474
diagnose wad debug save-http-req-crash disable	3474
diagnose wad debug save-http-req-crash enable	3475
diagnose wad debug show	3475
diagnose wad dev	3475
diagnose wad dev fcnacd	3475
diagnose wad dev fcnacd delete	3475
diagnose wad dev fcnacd ip-err	3475
diagnose wad dev fcnacd uid-err	3476
diagnose wad dev fcnacd update	3476
diagnose wad dev query-by	3476
diagnose wad dev query-by ipv4	3476
diagnose wad dev query-by ipv6	3476
diagnose wad dev query-by uid	3476
diagnose wad dev-vuln	3477
diagnose wad dev-vuln query	3477
diagnose wad dev-vuln query-by-id	3477
diagnose wad dev-vuln query-ftgd	3477
diagnose wad filter	3477
diagnose wad filter clear	3477
diagnose wad filter dport	3478
diagnose wad filter drop-unknown-session	3478
diagnose wad filter dst	3478
diagnose wad filter dst6	3478
diagnose wad filter explicit-policy	3479
diagnose wad filter firewall-policy	3479
diagnose wad filter list	3479
diagnose wad filter negate	3479
diagnose wad filter process-id	3480
diagnose wad filter process-id-by-src	3480
diagnose wad filter process-type	3480
diagnose wad filter protocol	3480
diagnose wad filter proxy-policy-list-increment	3481
diagnose wad filter sport	3481
diagnose wad filter src	3481
diagnose wad filter src6	3482
diagnose wad filter vd	3482
diagnose wad health	3482
diagnose wad health debug	3482
diagnose wad health fs	3482
diagnose wad health worker	3483

diagnose wad history	3483
diagnose wad history clear	3483
diagnose wad history list	3483
diagnose wad kxp	3483
diagnose wad kxp clear	3484
diagnose wad kxp list	3484
diagnose wad memory	3484
diagnose wad memory monitor	3484
diagnose wad memory monitor disable	3484
diagnose wad memory monitor enable	3484
diagnose wad memory monitor interval	3485
diagnose wad memory monitor list	3485
diagnose wad memory monitor max-report-files	3485
diagnose wad memory monitor mem-threshold-red	3485
diagnose wad memory overused	3485
diagnose wad memory report	3486
diagnose wad memory sum	3486
diagnose wad memory track	3486
diagnose wad memory workers	3486
diagnose wad process	3486
diagnose wad process YouTube-filter-cache-service	3487
diagnose wad process algo	3489
diagnose wad process byte-cache	3491
diagnose wad process cache-service-cs	3493
diagnose wad process cache-service-db	3495
diagnose wad process cert-inspection	3497
diagnose wad process cert-manager	3499
diagnose wad process config-notify	3501
diagnose wad process debug	3503
diagnose wad process dev-vuln	3505
diagnose wad process dispatcher	3507
diagnose wad process informer	3509
diagnose wad process inline-ips-pktlog	3511
diagnose wad process manager	3513
diagnose wad process object-cache	3515
diagnose wad process reverse-connector	3517
diagnose wad process staled-worker	3519
diagnose wad process user-info	3521
diagnose wad process user-info-history	3523
diagnose wad process worker	3525
diagnose wad report	3527
diagnose wad report policy	3527
diagnose wad report session	3527
diagnose wad report user	3527
diagnose wad restore	3527
diagnose wad restore cdn-rules	3527
diagnose wad restore cdn-rules all	3528
diagnose wad session	3528
diagnose wad session clear	3528

diagnose wad session list	3528
diagnose wad session list-http2	3528
diagnose wad stats	3528
diagnose wad stats algo	3529
diagnose wad stats algo.antiphish	3529
diagnose wad stats algo.casb	3529
diagnose wad stats algo.dev_info	3529
diagnose wad stats algo.dev_type	3529
diagnose wad stats algo.fw_policy	3530
diagnose wad stats algo.icap_client	3530
diagnose wad stats algo.ips	3530
diagnose wad stats algo.ips_builder	3530
diagnose wad stats algo.proc_common	3531
diagnose wad stats algo.sec_prof	3531
diagnose wad stats algo.ssl	3531
diagnose wad stats algo.url_filter	3531
diagnose wad stats cache_service	3532
diagnose wad stats cache_service.proc_common	3532
diagnose wad stats cache_service.tcp	3532
diagnose wad stats cic	3532
diagnose wad stats cic.proc_common	3532
diagnose wad stats cmgr	3533
diagnose wad stats cmgr.cert_cache	3533
diagnose wad stats cmgr.cert_service	3533
diagnose wad stats cmgr.dns_req	3533
diagnose wad stats cmgr.http_engine	3534
diagnose wad stats cmgr.proc_common	3534
diagnose wad stats cmgr.quic	3534
diagnose wad stats cmgr.ssl	3534
diagnose wad stats cmgr.tcp	3535
diagnose wad stats common	3535
diagnose wad stats common.dc_ad_dns	3535
diagnose wad stats common.diag	3535
diagnose wad stats common.sched	3535
diagnose wad stats common.ses_stats	3536
diagnose wad stats common.waps	3536
diagnose wad stats config	3536
diagnose wad stats config.proc_common	3536
diagnose wad stats config.stream_scan	3537
diagnose wad stats debug	3537
diagnose wad stats debug.crash_handler	3537
diagnose wad stats debug.proc_common	3537
diagnose wad stats dev_vuln	3538
diagnose wad stats dev_vuln.dns_req	3538
diagnose wad stats dev_vuln.proc_common	3538
diagnose wad stats dev_vuln.ssl	3538
diagnose wad stats dev_vuln.tcp	3538
diagnose wad stats dispatcher	3539
diagnose wad stats dispatcher.cifs	3539

diagnose wad stats dispatcher.dns_proxy	3539
diagnose wad stats dispatcher.proc_common	3539
diagnose wad stats dispatcher.ssh	3540
diagnose wad stats dispatcher.tcp	3540
diagnose wad stats dispatcher.tunnel	3540
diagnose wad stats informer	3540
diagnose wad stats informer.dev_info	3541
diagnose wad stats informer.dev_type	3541
diagnose wad stats informer.proc_common	3541
diagnose wad stats informer.usr_info_common	3541
diagnose wad stats informer.ztna_jwt	3541
diagnose wad stats mgr	3542
diagnose wad stats mgr.proc_common	3542
diagnose wad stats uih	3542
diagnose wad stats uih.proc_common	3542
diagnose wad stats usr_info	3543
diagnose wad stats usr_info.dev_info	3543
diagnose wad stats usr_info.dev_type	3543
diagnose wad stats usr_info.dns_req	3543
diagnose wad stats usr_info.proc_common	3544
diagnose wad stats usr_info.ssl	3544
diagnose wad stats usr_info.tcp	3544
diagnose wad stats usr_info.usr_info_common	3544
diagnose wad stats vfcs	3544
diagnose wad stats vfcs.proc_common	3545
diagnose wad stats worker	3545
diagnose wad stats worker.antiphish	3545
diagnose wad stats worker.app_mgr	3545
diagnose wad stats worker.casb	3546
diagnose wad stats worker.casb_eng	3546
diagnose wad stats worker.cert_cache	3546
diagnose wad stats worker.cifs	3546
diagnose wad stats worker.config_delta	3547
diagnose wad stats worker.conn_pool	3547
diagnose wad stats worker.dev_info	3547
diagnose wad stats worker.dev_type	3547
diagnose wad stats worker.digest	3547
diagnose wad stats worker.dns_proxy	3548
diagnose wad stats worker.dns_req	3548
diagnose wad stats worker.fast_match	3548
diagnose wad stats worker.fw_policy	3548
diagnose wad stats worker.hauth_uid_cache	3549
diagnose wad stats worker.http_engine	3549
diagnose wad stats worker.http_ffbk	3549
diagnose wad stats worker.http_scan	3549
diagnose wad stats worker.http_srv_selector	3550
diagnose wad stats worker.icap_client	3550
diagnose wad stats worker.icap_parser	3550
diagnose wad stats worker.icap_remote_server	3550

diagnose wad stats worker.infection_cache	3550
diagnose wad stats worker.ipseng	3551
diagnose wad stats worker.pol_test	3551
diagnose wad stats worker.policy_profile	3551
diagnose wad stats worker.proc_common	3551
diagnose wad stats worker.protos	3552
diagnose wad stats worker.quic	3552
diagnose wad stats worker.saml	3552
diagnose wad stats worker.sec_prof	3552
diagnose wad stats worker.ssh	3553
diagnose wad stats worker.ssl	3553
diagnose wad stats worker.sysmem	3553
diagnose wad stats worker.tcp	3553
diagnose wad stats worker.traffic_mirror	3553
diagnose wad stats worker.tunnel	3554
diagnose wad stats worker.url_filter	3554
diagnose wad stats worker.usr_info_common	3554
diagnose wad stats worker.vs_cert_cache	3554
diagnose wad stats worker.ztna_jwt	3555
diagnose wad stream-scan	3555
diagnose wad stream-scan av-intf	3555
diagnose wad stream-scan av-intf disable	3555
diagnose wad stream-scan av-intf enable	3555
diagnose wad stream-scan av-test	3556
diagnose wad toggle	3556
diagnose wad tunnel	3556
diagnose wad tunnel clear	3556
diagnose wad tunnel list	3556
diagnose wad uih	3557
diagnose wad uih chart	3557
diagnose wad uih chart range	3557
diagnose wad uih chart summary	3557
diagnose wad user	3557
diagnose wad user clear	3557
diagnose wad user device	3558
diagnose wad user domain-controller	3558
diagnose wad user domain-controller dns	3558
diagnose wad user domain-controller dns list	3558
diagnose wad user domain-controller dns test	3558
diagnose wad user exchange	3558
diagnose wad user exchange get-matches	3559
diagnose wad user exchange query-rows	3559
diagnose wad user exchange reset	3559
diagnose wad user exchange resolve-names	3559
diagnose wad user exchange test-auto-discover	3559
diagnose wad user list	3559
diagnose wad webcache	3560
diagnose wad webcache clear	3560
diagnose wad webcache list	3560

diagnose wad worker	3560
diagnose wad worker async-ut	3560
diagnose wad worker avscan	3561
diagnose wad worker avscan clear	3561
diagnose wad worker avscan list	3561
diagnose wad worker bytcache	3561
diagnose wad worker bytcache clear	3561
diagnose wad worker bytcache flush	3561
diagnose wad worker bytcache stats	3562
diagnose wad worker bytcache toggle	3562
diagnose wad worker bytcache toggle all	3562
diagnose wad worker bytcache toggle config	3562
diagnose wad worker bytcache toggle create	3563
diagnose wad worker bytcache toggle read	3563
diagnose wad worker cookie	3563
diagnose wad worker cookie clear-cors	3563
diagnose wad worker cookie list-cors	3563
diagnose wad worker cookie map	3564
diagnose wad worker filter	3564
diagnose wad worker filter clear	3564
diagnose wad worker filter list	3564
diagnose wad worker memcache	3564
diagnose wad worker memcache clear	3564
diagnose wad worker memcache flush	3565
diagnose wad worker memcache stats	3565
diagnose wad worker memcache toggle	3565
diagnose wad worker memcache toggle all	3565
diagnose wad worker memcache toggle config	3565
diagnose wad worker memcache toggle create	3566
diagnose wad worker memcache toggle read	3566
diagnose wad worker peer	3566
diagnose wad worker peer clear	3566
diagnose wad worker peer list	3566
diagnose wad worker policy	3567
diagnose wad worker policy clear	3567
diagnose wad worker policy list	3567
diagnose wad worker restart	3567
diagnose wad worker saml	3567
diagnose wad worker scripts	3568
diagnose wad worker scripts clear	3568
diagnose wad worker scripts list	3568
diagnose wad worker webcache	3568
diagnose wad worker webcache clear	3568
diagnose wad worker webcache flush	3568
diagnose wad worker webcache stats	3569
diagnose wad worker webcache summary	3569
diagnose wad worker webcache toggle	3569
diagnose wad worker webcache toggle abort	3569
diagnose wad worker webcache toggle add_ref	3569

diagnose wad worker webcache toggle all	3570
diagnose wad worker webcache toggle append	3570
diagnose wad worker webcache toggle config	3570
diagnose wad worker webcache toggle create	3570
diagnose wad worker webcache toggle read	3571
diagnose wad worker webcache toggle remove	3571
diagnose wad worker webcache toggle resolve	3571
diagnose wad worker webcache toggle update	3571
diagnose wadbd	3572
diagnose wadbd clear	3572
diagnose wadbd restart	3572
diagnose wadbd stats	3572
diagnose waf	3572
diagnose waf dump	3573
diagnose waf info	3573
diagnose webfilter bword	3573
diagnose webfilter bword matchfilter	3573
diagnose webfilter fortiguard	3573
diagnose webfilter fortiguard cache	3574
diagnose webfilter fortiguard cache dump	3574
diagnose webfilter fortiguard cache obs	3574
diagnose webfilter fortiguard cache prefix	3574
diagnose webfilter fortiguard cache tree	3575
diagnose webfilter fortiguard cache ttl	3575
diagnose webfilter fortiguard override	3575
diagnose webfilter fortiguard override all-admin-override	3575
diagnose webfilter fortiguard override all-user-override	3575
diagnose webfilter fortiguard override all-warning	3575
diagnose webfilter fortiguard override obs	3576
diagnose webfilter fortiguard override statistics	3576
diagnose webfilter fortiguard statistics	3576
diagnose webfilter fortiguard statistics flush	3576
diagnose webfilter fortiguard statistics list	3576
diagnose webfilter quota	3576
diagnose webfilter quota list	3577
diagnose webfilter stats	3577
diagnose webfilter stats clear	3577
diagnose webfilter stats list	3577
diagnose web-ui	3577
diagnose web-ui api-cache	3578
diagnose web-ui api-cache statistic	3578
diagnose web-ui api-stats	3578
diagnose web-ui api-stats disable	3579
diagnose web-ui api-stats enable	3579
diagnose web-ui api-stats list	3579
diagnose web-ui api-stats reset	3579
diagnose web-ui api-stats status	3579
diagnose web-ui backtrace	3579

diagnose web-ui backtrace clear	3580
diagnose web-ui backtrace disable	3580
diagnose web-ui backtrace enable	3580
diagnose web-ui backtrace httpsd	3580
diagnose web-ui backtrace status	3580
diagnose web-ui cache	3581
diagnose web-ui cache disable	3581
diagnose web-ui cache enable	3581
diagnose web-ui local-process-guard	3581
diagnose web-ui local-process-guard disable	3581
diagnose web-ui local-process-guard enable	3581
diagnose web-ui local-process-guard status	3582
diagnose web-ui localization	3582
diagnose web-ui localization disable	3582
diagnose web-ui localization enable	3582
diagnose wireless-controller	3582
diagnose wireless-controller wlac	3582
diagnose wireless-controller wlac_hlp	3583
diagnose wpa	3583
diagnose wpa wpad	3584
CLI execute commands	3585
execute api-user	3587
execute api-user generate-key	3588
execute auto-script	3588
execute auto-script backup ftp	3588
execute auto-script backup tftp	3589
execute auto-script delete	3589
execute auto-script result	3589
execute auto-script start	3589
execute auto-script status	3590
execute auto-script stop	3590
execute auto-script stopall	3590
execute azure	3590
execute azure vwan-payg-billing status	3590
execute azure vwan-payg-billing usage	3591
execute azure vwan-slb pull	3591
execute azure vwan-slb show	3591
execute backup	3591
execute backup config flash	3592
execute backup config ftp	3592
execute backup config management-station	3593
execute backup config sftp	3593
execute backup config tftp	3593
execute backup disk alllogs ftp	3594
execute backup disk alllogs tftp	3594
execute backup disk ipsarchives ftp	3594
execute backup disk ipsarchives tftp	3594
execute backup disk log ftp	3595

execute backup disk log tftp	3595
execute backup full-config ftp	3595
execute backup full-config sftp	3596
execute backup full-config tftp	3596
execute backup ipsuserdefsig ftp	3597
execute backup ipsuserdefsig tftp	3597
execute backup memory alllogs ftp	3597
execute backup memory alllogs tftp	3597
execute backup memory log ftp	3598
execute backup memory log tftp	3598
execute backup obfuscated-config ftp	3598
execute backup obfuscated-config management-station	3599
execute backup obfuscated-config sftp	3599
execute backup obfuscated-config tftp	3599
execute backup obfuscated-full-config ftp	3600
execute backup obfuscated-full-config sftp	3600
execute backup obfuscated-full-config tftp	3601
execute backup obfuscated-yaml-config ftp	3601
execute backup obfuscated-yaml-config tftp	3601
execute backup yaml-config ftp	3602
execute backup yaml-config tftp	3602
execute batch	3602
execute batch end	3603
execute batch lastlog	3603
execute batch start	3603
execute batch status	3603
execute central-mgmt	3603
execute central-mgmt register-device	3603
execute central-mgmt set-mgmt-id	3604
execute central-mgmt unregister-device	3604
execute cfg	3604
execute cfg reload	3604
execute cfg save	3605
execute clear	3605
execute clear system arp table	3605
execute clear-admin-password-history	3605
execute clear-user-password-history	3605
execute cli	3606
execute cli check-template-status	3606
execute cli status-msg-only	3606
execute cloud-service	3606
execute cloud-service gen-jwt-as-token	3607
execute cloud-service list	3607
execute cloud-service manual-gen-jwt-as-token	3607
execute config-transaction	3607
execute config-transaction abort	3608
execute config-transaction commit	3608
execute config-transaction start	3608

execute cpu	3608
execute cpu add	3608
execute cpu show	3609
execute date	3609
execute device-upgrade	3609
execute device-upgrade cancel	3609
execute device-upgrade immediate	3610
execute dhcp	3610
execute dhcp lease-clear	3610
execute dhcp lease-list	3611
execute dhcp6	3611
execute dhcp6 lease-clear	3611
execute dhcp6 lease-list	3611
execute disconnect-admin-session	3612
execute disk	3612
execute disk format	3612
execute disk list	3612
execute disk scan	3612
execute enter	3613
execute erase-disk	3613
execute extender	3613
execute extender delete-fortiextender-image	3614
execute extender install-forticloud-mdm-package	3614
execute extender install-forticloud-os-image	3614
execute extender list-fortiextender-image	3614
execute extender lte-carrier add	3614
execute extender lte-carrier del	3615
execute extender lte-simmap add	3615
execute extender lte-simmap del	3615
execute extender push-fortiextender-image	3616
execute extender push-fortiextender-stage-image	3616
execute extender query-forticloud-mdmpkg-image	3616
execute extender query-forticloud-os-image	3617
execute extender reset-fortiextender	3617
execute extender restart-fortiextender-daemon	3617
execute extender upload-fortiextender-image ftp	3617
execute extender upload-fortiextender-image tftp	3618
execute fabric-vpn	3618
execute fabric-vpn flush-setup	3618
execute fabric-vpn update-setup	3618
execute factoryreset	3618
execute factoryreset2	3619
execute factoryreset-for-central-management	3619
execute factoryreset-shutdown	3619
execute fctems	3620
execute fctems is-verified	3620
execute fctems unverify	3620

execute fctems verify	3620
execute federated-upgrade	3621
execute federated-upgrade cancel	3621
execute federated-upgrade initialize	3621
execute federated-upgrade quick-fortigate-upgrade	3621
execute federated-upgrade quick-full-upgrade	3622
execute federated-upgrade restart	3622
execute federated-upgrade safe-cancel	3622
execute federated-upgrade status	3622
execute fips	3623
execute fips tftp-drbg-entropy-source	3623
execute fips tftp-test-vectors	3623
execute firewall	3623
execute firewall ssh generate local-ca	3624
execute firewall ssh generate local-key	3624
execute formatlogdisk	3624
execute forticarrier-license	3624
execute forticloud-sandbox	3625
execute forticloud-sandbox region	3625
execute forticloud-sandbox update	3625
execute fortiguard-log	3625
execute fortiguard-log certificate-activation	3625
execute fortiguard-log migration	3626
execute fortiguard-log update	3626
execute fortiguard-message	3626
execute fortiguard-message add	3626
execute fortiguard-message info	3626
execute fortiguard-message update	3627
execute fortimanager	3627
execute fortimanager fetch	3627
execute fortimanager register	3627
execute fortitoken	3627
execute fortitoken activate	3628
execute fortitoken import ftp	3629
execute fortitoken import tftp	3629
execute fortitoken import usb	3629
execute fortitoken import-sn-file	3629
execute fortitoken sync	3630
execute fortitoken-cloud	3630
execute fortitoken-cloud migrate-ftm	3630
execute fortitoken-cloud new	3631
execute fortitoken-cloud show	3631
execute fortitoken-cloud sync	3631
execute fortitoken-cloud trial	3631
execute fortitoken-cloud update	3631
execute fortitoken-mobile	3632
execute fortitoken-mobile import	3632
execute fortitoken-mobile poll	3632

execute fortitoken-mobile provision	3632
execute fortitoken-mobile renew	3632
execute fsso	3633
execute fsso refresh	3633
execute gen-token	3633
execute ha	3634
execute ha disconnect	3634
execute ha failover set	3634
execute ha failover status	3635
execute ha failover unset	3635
execute ha manage	3635
execute ha synchronize	3635
execute interface	3636
execute interface dhcp6client-renew	3636
execute interface dhcpclient-renew	3636
execute interface pppoe-reconnect	3636
execute internet-service4	3637
execute internet-service4 refresh	3637
execute internet-service6	3637
execute internet-service6 refresh	3637
execute ipam	3637
execute ipam create-dhcp-server	3637
execute iscsi	3638
execute iscsi login	3638
execute iscsi logout	3638
execute iscsi show	3638
execute kmip	3639
execute kmip create	3639
execute kmip destroy	3639
execute kmip get	3640
execute kmip locate	3640
execute kmip rekey	3640
execute log	3640
execute log backup ftp	3641
execute log backup local	3642
execute log backup tftp	3642
execute log chroot	3642
execute log delete	3642
execute log delete-all	3643
execute log detail	3643
execute log display	3643
execute log filter category	3643
execute log filter device	3643
execute log filter dump	3644
execute log filter field	3644
execute log filter free-style	3644
execute log filter ha-member	3645
execute log filter local-search-mode	3645

execute log filter max-checklines	3645
execute log filter pre-fetch-pages	3645
execute log filter reset	3645
execute log filter start-line	3646
execute log filter view-lines	3646
execute log flush-cache	3646
execute log flush-cache-all	3646
execute log fortianalyzer manual-failover	3646
execute log fortianalyzer test-connectivity	3647
execute log fortianalyzer-cloud test-connectivity	3647
execute log fortianalyzer2 manual-failover	3647
execute log fortianalyzer3 manual-failover	3647
execute log fortiguard test-connectivity	3647
execute log list	3647
execute log raw-backup ftp	3648
execute log raw-backup tftp	3648
execute log restore	3648
execute log roll	3649
execute log shift-time	3649
execute log upload	3649
execute log upload-progress	3649
execute mem	3649
execute mem add	3649
execute mrouter	3650
execute mrouter clear dense-routes	3650
execute mrouter clear igmp-group	3650
execute mrouter clear igmp-interface	3651
execute mrouter clear multicast-routes	3651
execute mrouter clear sparse-mode-bsr	3651
execute mrouter clear sparse-routes	3651
execute mrouter clear statistics	3652
execute mrouter6	3652
execute mrouter6 clear mld	3652
execute mrouter6 clear sparse-routes	3652
execute nsx	3653
execute nsx group delete	3653
execute nsx group import	3653
execute nsx group list	3654
execute oqs	3654
execute ping	3654
execute ping6	3654
execute ping6-options	3655
execute ping6-options adaptive-ping	3655
execute ping6-options data-size	3655
execute ping6-options interface	3656
execute ping6-options interval	3656
execute ping6-options pattern	3656
execute ping6-options repeat-count	3656

execute ping6-options reset	3656
execute ping6-options source6	3657
execute ping6-options timeout	3657
execute ping6-options tos	3657
execute ping6-options ttl	3657
execute ping6-options use-sdwan	3658
execute ping6-options validate-reply	3658
execute ping6-options view-settings	3658
execute ping6-options vrf	3658
execute ping-options	3658
execute ping-options adaptive-ping	3659
execute ping-options data-size	3659
execute ping-options df-bit	3659
execute ping-options interface	3660
execute ping-options interval	3660
execute ping-options pattern	3660
execute ping-options repeat-count	3660
execute ping-options reset	3661
execute ping-options source	3661
execute ping-options timeout	3661
execute ping-options tos	3661
execute ping-options ttl	3661
execute ping-options use-sdwan	3662
execute ping-options validate-reply	3662
execute ping-options view-settings	3662
execute ping-options vrf	3662
execute policy-packet-capture	3663
execute policy-packet-capture delete-all	3663
execute reboot	3663
execute replace-device	3663
execute replace-device fortiaip	3663
execute replace-device fortiswitch	3664
execute report	3664
execute report flush-cache	3664
execute report recreate-db	3664
execute report run	3665
execute report sandbox-status	3665
execute report-config	3665
execute report-config reset	3665
execute restore	3666
execute restore av ftp	3666
execute restore av tftp	3667
execute restore config dhcp	3667
execute restore config flash	3667
execute restore config ftp	3668
execute restore config management-station normal	3668
execute restore config management-station script	3668
execute restore config management-station template	3668

execute restore config tftp	3669
execute restore image flash	3669
execute restore image ftp	3669
execute restore image management-station	3670
execute restore image tftp	3670
execute restore image url	3670
execute restore ips ftp	3670
execute restore ips tftp	3671
execute restore ipsuserdefsig ftp	3671
execute restore ipsuserdefsig tftp	3671
execute restore manual-license ftp	3672
execute restore manual-license tftp	3672
execute restore other-objects ftp	3672
execute restore other-objects tftp	3673
execute restore script ftp	3673
execute restore script lastlog	3673
execute restore script scp	3674
execute restore script tftp	3674
execute restore vmlicense ftp	3674
execute restore vmlicense tftp	3675
execute revision	3675
execute revision delete config	3675
execute revision delete image	3675
execute revision list config	3676
execute revision list image	3676
execute router	3676
execute router clear bfd session	3676
execute router clear bgp all	3677
execute router clear bgp as	3677
execute router clear bgp dampening	3677
execute router clear bgp external	3677
execute router clear bgp flap-statistics	3677
execute router clear bgp group	3678
execute router clear bgp ip	3678
execute router clear bgp ipv6	3678
execute router clear ospf process	3678
execute router clear ospf6 process	3678
execute router restart	3678
execute sdn	3679
execute sdn tag add nsx	3679
execute sdn tag remove nsx	3679
execute sdn-vpn	3679
execute sdn-vpn discover aws-tgw	3680
execute sdn-vpn discover aws-vgw	3680
execute send-fds-statistics	3680
execute send-fmg-list	3680
execute set	3681
execute set system session filter clear all	3681

execute set system session filter clear dport	3682
execute set system session filter clear dst	3682
execute set system session filter clear duration	3682
execute set system session filter clear expire	3682
execute set system session filter clear policy	3682
execute set system session filter clear proto	3682
execute set system session filter clear sport	3683
execute set system session filter clear src	3683
execute set system session filter clear vd	3683
execute set system session filter dport	3683
execute set system session filter dst	3683
execute set system session filter duration	3684
execute set system session filter expire	3684
execute set system session filter list	3684
execute set system session filter negate dport	3684
execute set system session filter negate dst	3684
execute set system session filter negate duration	3685
execute set system session filter negate expire	3685
execute set system session filter negate policy	3685
execute set system session filter negate proto	3685
execute set system session filter negate sport	3685
execute set system session filter negate src	3685
execute set system session filter negate vd	3686
execute set system session filter policy	3686
execute set system session filter proto	3686
execute set system session filter sport	3686
execute set system session filter src	3687
execute set system session filter vd	3687
execute shutdown	3687
execute speed-test	3687
execute speed-test-custom	3688
execute speed-test-ipsec	3688
execute speed-test-options	3688
execute speed-test-options blksize	3689
execute speed-test-options burst	3689
execute speed-test-options ctrl-port	3689
execute speed-test-options duration	3690
execute speed-test-options get-token	3690
execute speed-test-options max-down	3690
execute speed-test-options max-up	3690
execute speed-test-options protocol	3691
execute speed-test-options reset	3691
execute speed-test-options reset-token	3691
execute speed-test-options server-port	3691
execute speed-test-options set-shaper	3691
execute speed-test-options show	3692
execute speed-test-options tos	3692
execute speed-test-server	3692

execute speed-test-server download	3692
execute speed-test-server list	3692
execute ssh	3693
execute ssh6	3693
execute ssh6-options	3693
execute ssh6-options interface	3693
execute ssh6-options reset	3694
execute ssh6-options source6	3694
execute ssh6-options view-settings	3694
execute ssh-options	3694
execute ssh-options interface	3694
execute ssh-options reset	3695
execute ssh-options source	3695
execute ssh-options view-settings	3695
execute ssh-regen-keys	3695
execute switch-controller	3695
execute switch-controller custom-command	3697
execute switch-controller diagnose-connection	3697
execute switch-controller diagnose-connection-v6	3698
execute switch-controller flapguard reset	3698
execute switch-controller get-conn-status	3698
execute switch-controller get-physical-conn dot	3698
execute switch-controller get-physical-conn standard	3699
execute switch-controller get-sync-status all	3699
execute switch-controller get-sync-status group	3699
execute switch-controller get-sync-status serial	3699
execute switch-controller get-sync-status switch-id	3700
execute switch-controller get-upgrade-status	3700
execute switch-controller ssh	3700
execute switch-controller switch-action 802-1X clear-auth-mac	3700
execute switch-controller switch-action 802-1X clear-auth-port	3701
execute switch-controller switch-action bpdu-guard reset	3701
execute switch-controller switch-action cable-diag	3701
execute switch-controller switch-action factory-reset	3701
execute switch-controller switch-action flow-tracking delete-flows-all	3702
execute switch-controller switch-action flow-tracking expire-flows-all	3702
execute switch-controller switch-action igmp-snoop clear-learned	3702
execute switch-controller switch-action loop-guard reset	3702
execute switch-controller switch-action mac-device-reset dynamic	3703
execute switch-controller switch-action mac-device-reset nac	3703
execute switch-controller switch-action mac-limit-violation reset all	3703
execute switch-controller switch-action mac-limit-violation reset interface	3704
execute switch-controller switch-action mac-limit-violation reset vlan	3704
execute switch-controller switch-action mclag stats clear icl	3704
execute switch-controller switch-action mclag stats clear mlag	3704
execute switch-controller switch-action physical-ports led-flash switch-	
group	3705
execute switch-controller switch-action physical-ports led-flash switch-id ...	3705

execute switch-controller switch-action physical-ports led-flash tier1	3705
execute switch-controller switch-action physical-ports led-flash tier2plus	3706
execute switch-controller switch-action poe reset	3706
execute switch-controller switch-action restart delay all	3706
execute switch-controller switch-action restart delay switch-group	3706
execute switch-controller switch-action restart delay switch-id	3707
execute switch-controller switch-action restart swtp all	3707
execute switch-controller switch-action restart swtp switch-group	3707
execute switch-controller switch-action restart swtp switch-id	3707
execute switch-controller switch-action set-standalone	3708
execute switch-controller switch-action sticky-mac delete-unsaved all	3708
execute switch-controller switch-action sticky-mac delete-unsaved	
interface	3708
execute switch-controller switch-action sticky-mac save all	3709
execute switch-controller switch-action sticky-mac save interface	3709
execute switch-controller switch-software cancel all	3709
execute switch-controller switch-software cancel switch-group	3709
execute switch-controller switch-software cancel switch-id	3710
execute switch-controller switch-software delete	3710
execute switch-controller switch-software list-available	3710
execute switch-controller switch-software stage all	3710
execute switch-controller switch-software stage switch-group	3710
execute switch-controller switch-software stage switch-id	3711
execute switch-controller switch-software upgrade	3711
execute switch-controller switch-software upload ftp	3711
execute switch-controller switch-software upload tftp	3712
execute switch-controller virtual-port-pool request	3712
execute switch-controller virtual-port-pool return	3712
execute switch-controller virtual-port-pool show	3713
execute switch-controller virtual-port-pool show-by-pool	3713
execute switch-controller virtual-port-pool show-by-property	3713
execute switch-controller virtual-port-pool show-by-tag	3713
execute sync-IPSec	3713
execute sync-session	3714
execute system	3714
execute system custom-language import	3714
execute system fortisandbox test-connectivity	3714
execute tac	3715
execute tac report	3715
execute telnet	3715
execute telnet-options	3715
execute telnet-options interface	3715
execute telnet-options reset	3716
execute telnet-options source	3716
execute telnet-options view-settings	3716
execute test	3716
execute test tftp-analytics-report	3716
execute time	3717

execute traceroute	3717
execute traceroute-options	3717
execute traceroute-options device	3718
execute traceroute-options queries	3718
execute traceroute-options reset	3718
execute traceroute-options source	3718
execute traceroute-options use-sdwan	3718
execute traceroute-options view-settings	3719
execute traceroute-options vrf	3719
execute tracert6	3719
execute update-av	3719
execute update-eip	3719
execute update-external-resource	3720
execute update-ffdb-on-demand	3720
execute update-geo-ip	3720
execute update-ips	3720
execute update-now	3720
execute update-src-vis	3721
execute upd-vd-license	3721
execute upload	3721
execute upload config ftp	3721
execute upload config tftp	3722
execute upload image ftp	3722
execute upload image tftp	3723
execute upload report-img ftp	3723
execute upload report-img tftp	3723
execute vm-license	3724
execute vm-license-options	3724
execute vm-license-options account-id	3724
execute vm-license-options account-password	3724
execute vm-license-options count	3725
execute vm-license-options government	3725
execute vm-license-options interval	3725
execute vm-license-options proxy	3725
execute vm-license-options reset	3726
execute vm-license-options show	3726
execute vm-license-options token	3726
execute vpn	3726
execute vpn certificate ca export tftp	3727
execute vpn certificate ca import auto	3727
execute vpn certificate ca import bundle	3728
execute vpn certificate ca import est	3728
execute vpn certificate ca import tftp	3729
execute vpn certificate crl import auto	3729
execute vpn certificate ems_ca import tftp	3729
execute vpn certificate hsm-local gch-get-versions	3729
execute vpn certificate hsm-local status	3730

execute vpn certificate hsm-local verify	3730
execute vpn certificate local export tftp	3730
execute vpn certificate local generate cmp-ec	3730
execute vpn certificate local generate cmp-rsa	3731
execute vpn certificate local generate default-gui-mgmt-cert	3732
execute vpn certificate local generate default-ssl-ca	3732
execute vpn certificate local generate default-ssl-ca-untrusted	3732
execute vpn certificate local generate default-ssl-key-certs	3732
execute vpn certificate local generate default-ssl-serv-key	3733
execute vpn certificate local generate ec	3733
execute vpn certificate local generate est	3734
execute vpn certificate local generate rsa	3734
execute vpn certificate local import tftp	3735
execute vpn certificate local verify	3735
execute vpn certificate remote export tftp	3736
execute vpn certificate remote import tftp	3736
execute vpn ikecrypt dhperf compute	3736
execute vpn ikecrypt dhperf generate	3737
execute vpn ipsec tunnel down	3737
execute vpn ipsec tunnel up	3737
execute vpn sslvpn del-all	3737
execute vpn sslvpn del-tunnel	3738
execute vpn sslvpn del-web	3738
execute vpn sslvpn list	3738
execute wake-on-lan	3738
execute webcache	3739
execute webcache delete regular-expression	3739
execute webcache delete simple-string	3739
execute webcache delete status	3740
execute webcache delete wildcard	3740
execute webfilter	3740
execute webfilter quota-reset	3740
execute wireless-controller	3740
execute wireless-controller create-sae-pk	3741
execute wireless-controller delete-wtp-image	3741
execute wireless-controller hs20-icon backup-icon ftp	3742
execute wireless-controller hs20-icon backup-icon tftp	3742
execute wireless-controller hs20-icon delete-hs-icon	3742
execute wireless-controller hs20-icon list-hs-icon	3742
execute wireless-controller hs20-icon upload-icon ftp	3743
execute wireless-controller hs20-icon upload-icon tftp	3743
execute wireless-controller led-blink	3743
execute wireless-controller list-wtp-image	3743
execute wireless-controller mpsk-key create-keys	3744
execute wireless-controller push-wtp-image	3744
execute wireless-controller reset-wtp	3744
execute wireless-controller restart-acd	3745
execute wireless-controller rolling-wtp-upgrade	3745
execute wireless-controller spectral-scan	3745

execute wireless-controller upload-wtp-image ftp	3745
execute wireless-controller upload-wtp-image tftp	3746
Included devices	3747

Change Log

Date	Change Description
2025-04-16	Initial release of the FortiOS 7.6.3 CLI Reference.

FortiOS CLI reference

This document describes FortiOS 7.6.3 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI). For information on using the CLI, see the [FortiOS 7.6.3 Administration Guide](#), which contains information such as:

- [Connecting to the CLI](#)
- [CLI basics](#)
- [Command syntax](#)
- [Subcommands](#)
- [Permissions](#)

Availability of commands and options

Some FortiOS CLI commands and options are not available on all FortiGate units. The CLI displays an error message if you attempt to enter a command or option that is not available. You can use the question mark '?' to verify the commands and options that are available.

Commands and options may not be available for the following reasons:

FortiGate model

All commands are not available on all FortiGate models. For example, a hardware switch can be configured only on models which have the corresponding hardware switch chipset.

Hardware configuration

For example, settings like `mediatype` would only be available on units with SFPs.

FortiOS Carrier, FortiGate 5K/6K/7K, FortiGate with LTE, etc.

Commands for extended functionality are not available on all FortiGate models. The CLI Reference may not include all commands.

Command tree

Enter `tree` to display the entire FortiOS CLI command tree. To capture the full output, connect to your device using a terminal emulation program, such as PuTTY, and capture the output to a log file.

- To view all available commands, enter `tree`.
- To view a specific configuration branch of a tree, enter `tree <branch>`, for example: `tree system`.

- To view all available diagnose commands, enter `tree diagnose`.
- To view all available execute commands, enter `tree execute`.

CLI configuration commands

Use configuration commands to configure and manage a FortiGate unit from the command line interface (CLI).

alertemail

This section includes syntax for the following commands:

- [config alertemail setting on page 114](#)

config alertemail setting

Configure alert email settings.

```
config alertemail setting
  Description: Configure alert email settings.
  set FDS-license-expiring-warning [enable|disable]
  set FDS-update-logs [enable|disable]
  set FIPS-CC-errors [enable|disable]
  set FSSO-disconnect-logs [enable|disable]
  set HA-logs [enable|disable]
  set IPS-logs [enable|disable]
  set IPsec-errors-logs [enable|disable]
  set PPP-errors-logs [enable|disable]
  set admin-login-logs [enable|disable]
  set alert-interval {integer}
  set amc-interface-bypass-mode [enable|disable]
  set antivirus-logs [enable|disable]
  set configuration-changes-logs [enable|disable]
  set critical-interval {integer}
  set debug-interval {integer}
  set email-interval {integer}
  set emergency-interval {integer}
  set error-interval {integer}
  set filter-mode [category|threshold]
  set firewall-authentication-failure-logs [enable|disable]
  set fortiguard-log-quota-warning [enable|disable]
  set information-interval {integer}
  set local-disk-usage {integer}
  set log-disk-usage-warning [enable|disable]
  set mailto1 {string}
  set mailto2 {string}
  set mailto3 {string}
  set notification-interval {integer}
  set severity [emergency|alert|...]
  set ssh-logs [enable|disable]
  set sslvpn-authentication-errors-logs [enable|disable]
  set username {string}
  set violation-traffic-logs [enable|disable]
  set warning-interval {integer}
```

```
set webfilter-logs [enable|disable]
end
```

config alertemail setting

Parameter	Description	Type	Size	Default						
FDS-license-expiring-warning	Enable/disable FortiGuard license expiration warnings in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiGuard license expiration warnings in alert email.</td></tr><tr><td>disable</td><td>Disable FortiGuard license expiration warnings in alert email.</td></tr></table>	Option	Description	enable	Enable FortiGuard license expiration warnings in alert email.	disable	Disable FortiGuard license expiration warnings in alert email.			
Option	Description									
enable	Enable FortiGuard license expiration warnings in alert email.									
disable	Disable FortiGuard license expiration warnings in alert email.									
FDS-update-logs	Enable/disable FortiGuard update logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiGuard update logs in alert email.</td></tr><tr><td>disable</td><td>Disable FortiGuard update logs in alert email.</td></tr></table>	Option	Description	enable	Enable FortiGuard update logs in alert email.	disable	Disable FortiGuard update logs in alert email.			
Option	Description									
enable	Enable FortiGuard update logs in alert email.									
disable	Disable FortiGuard update logs in alert email.									
FIPS-CC-errors	Enable/disable FIPS and Common Criteria error logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FIPS and Common Criteria error logs in alert email.</td></tr><tr><td>disable</td><td>Disable FIPS and Common Criteria error logs in alert email.</td></tr></table>	Option	Description	enable	Enable FIPS and Common Criteria error logs in alert email.	disable	Disable FIPS and Common Criteria error logs in alert email.			
Option	Description									
enable	Enable FIPS and Common Criteria error logs in alert email.									
disable	Disable FIPS and Common Criteria error logs in alert email.									
FSSO-disconnect-logs	Enable/disable logging of FSSO collector agent disconnect.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging of FSSO collector agent disconnect.</td></tr><tr><td>disable</td><td>Disable logging of FSSO collector agent disconnect.</td></tr></table>	Option	Description	enable	Enable logging of FSSO collector agent disconnect.	disable	Disable logging of FSSO collector agent disconnect.			
Option	Description									
enable	Enable logging of FSSO collector agent disconnect.									
disable	Disable logging of FSSO collector agent disconnect.									
HA-logs	Enable/disable HA logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HA logs in alert email.</td></tr><tr><td>disable</td><td>Disable HA logs in alert email.</td></tr></table>	Option	Description	enable	Enable HA logs in alert email.	disable	Disable HA logs in alert email.			
Option	Description									
enable	Enable HA logs in alert email.									
disable	Disable HA logs in alert email.									
IPS-logs	Enable/disable IPS logs in alert email.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable IPS logs in alert email.		
	<i>disable</i>	Disable IPS logs in alert email.		
IPsec-errors-logs	Enable/disable IPsec error logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPsec error logs in alert email.		
	<i>disable</i>	Disable IPsec error logs in alert email.		
PPP-errors-logs	Enable/disable PPP error logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PPP error logs in alert email.		
	<i>disable</i>	Disable PPP error logs in alert email.		
admin-login-logs	Enable/disable administrator login/logout logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable administrator login/logout logs in alert email.		
	<i>disable</i>	Disable administrator login/logout logs in alert email.		
alert-interval	Alert alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	2
amc-interface-bypass-mode	Enable/disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.		
	<i>disable</i>	Disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.		
antivirus-logs	Enable/disable antivirus logs in alert email.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable antivirus logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable antivirus logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable antivirus logs in alert email.	<i>disable</i>	Disable antivirus logs in alert email.			
	Option	Description								
	<i>enable</i>	Enable antivirus logs in alert email.								
<i>disable</i>	Disable antivirus logs in alert email.									
configuration-changes-logs	Enable/disable configuration change logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable configuration change logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable configuration change logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable configuration change logs in alert email.	<i>disable</i>	Disable configuration change logs in alert email.			
	Option	Description								
	<i>enable</i>	Enable configuration change logs in alert email.								
<i>disable</i>	Disable configuration change logs in alert email.									
critical-interval	Critical alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	3						
debug-interval	Debug alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	60						
email-interval	Interval between sending alert emails (1 - 99999 min, default = 5).	integer	Minimum value: 1 Maximum value: 99999	5						
emergency-interval	Emergency alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	1						
error-interval	Error alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	5						
filter-mode	How to filter log messages that are sent to alert emails.	option	-	category						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>category</td><td>Filter based on category.</td></tr><tr><td>threshold</td><td>Filter based on severity.</td></tr></table>	Option	Description	category	Filter based on category.	threshold	Filter based on severity.			
	Option	Description								
	category	Filter based on category.								
threshold	Filter based on severity.									
firewall-authentication-failure-logs	Enable/disable firewall authentication failure logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable firewall authentication failure logs in alert email.</td></tr><tr><td>disable</td><td>Disable firewall authentication failure logs in alert email.</td></tr></table>	Option	Description	enable	Enable firewall authentication failure logs in alert email.	disable	Disable firewall authentication failure logs in alert email.			
	Option	Description								
	enable	Enable firewall authentication failure logs in alert email.								
disable	Disable firewall authentication failure logs in alert email.									
fortiguard-log-quota-warning	Enable/disable FortiCloud log quota warnings in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiCloud log quota warnings in alert email.</td></tr><tr><td>disable</td><td>Disable FortiCloud log quota warnings in alert email.</td></tr></table>	Option	Description	enable	Enable FortiCloud log quota warnings in alert email.	disable	Disable FortiCloud log quota warnings in alert email.			
	Option	Description								
	enable	Enable FortiCloud log quota warnings in alert email.								
disable	Disable FortiCloud log quota warnings in alert email.									
information-interval	Information alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	30						
local-disk-usage	Disk usage percentage at which to send alert email (1 - 99 percent, default = 75).	integer	Minimum value: 1 Maximum value: 99	75						
log-disk-usage-warning	Enable/disable disk usage warnings in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable disk usage warnings in alert email.</td></tr><tr><td>disable</td><td>Disable disk usage warnings in alert email.</td></tr></table>	Option	Description	enable	Enable disk usage warnings in alert email.	disable	Disable disk usage warnings in alert email.			
	Option	Description								
	enable	Enable disk usage warnings in alert email.								
disable	Disable disk usage warnings in alert email.									
mailto1	Email address to send alert email to (usually a system administrator) (max. 63 characters).	string	Maximum length: 63							
mailto2	Optional second email address to send alert email to (max. 63 characters).	string	Maximum length: 63							

Parameter	Description	Type	Size	Default																		
mailto3	Optional third email address to send alert email to (max. 63 characters).	string	Maximum length: 63																			
notification-interval	Notification alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	20																		
severity	Lowest severity level to log.	option	-	alert																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
ssh-logs	Enable/disable SSH logs in alert email.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable SSH logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSH logs in alert email.	<i>disable</i>	Disable SSH logs in alert email.															
Option	Description																					
<i>enable</i>	Enable SSH logs in alert email.																					
<i>disable</i>	Disable SSH logs in alert email.																					
sslvpn-authentication-errors-logs *	Enable/disable Agentless VPN authentication error logs in alert email.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Agentless VPN authentication error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable Agentless VPN authentication error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable Agentless VPN authentication error logs in alert email.	<i>disable</i>	Disable Agentless VPN authentication error logs in alert email.															
Option	Description																					
<i>enable</i>	Enable Agentless VPN authentication error logs in alert email.																					
<i>disable</i>	Disable Agentless VPN authentication error logs in alert email.																					
username	Name that appears in the From: field of alert emails (max. 63 characters).	string	Maximum length: 63																			
violation-traffic-logs	Enable/disable violation traffic logs in alert email.	option	-	disable																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable violation traffic logs in alert email.		
	<i>disable</i>	Disable violation traffic logs in alert email.		
warning-interval	Warning alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	10
webfilter-logs	Enable/disable web filter logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable web filter logs in alert email.		
	<i>disable</i>	Disable web filter logs in alert email.		

* This parameter may not exist in some models.

antivirus

This section includes syntax for the following commands:

- [config antivirus exempt-list on page 121](#)
- [config antivirus profile on page 122](#)
- [config antivirus quarantine on page 155](#)
- [config antivirus settings on page 159](#)

config antivirus exempt-list

Configure a list of hashes to be exempt from AV scanning.

```
config antivirus exempt-list
  Description: Configure a list of hashes to be exempt from AV scanning.
  edit <name>
    set comment {var-string}
    set hash {string}
    set hash-type [md5|sha1|...]
    set status [disable|enable]
  next
end
```

config antivirus exempt-list

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
hash	Hash value to be matched.	string	Maximum length: 64	
hash-type	Hash type.	option	-	sha1
	Option	Description		
	md5	MD5 hash value (32 characters in length).		
	sha1	SHA1 hash value (40 characters in length).		
	sha256	SHA256 hash value (64 characters in length).		
name	Table entry name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
status	Enable/disable table entry.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable AV exempt-list table entry.		
	<i>enable</i>	Enable AV exempt-list table entry.		

config antivirus profile

Configure AntiVirus profiles.

```

config antivirus profile
  Description: Configure AntiVirus profiles.
  edit <name>
    set analytics-accept-filetype {integer}
    set analytics-db [disable|enable]
    set analytics-ignore-filetype {integer}
    set av-virus-log [enable|disable]
    config cifs
      Description: Configure CIFS AntiVirus options.
      set archive-block {option1}, {option2}, ...
      set archive-log {option1}, {option2}, ...
      set av-scan [disable|block|...]
      set emulator [enable|disable]
      set external-blocklist [disable|block|...]
      set fortindr [disable|block|...]
      set fortisandbox [disable|block|...]
      set malware-stream [disable|block|...]
      set outbreak-prevention [disable|block|...]
      set quarantine [disable|enable]
    end
    set comment {var-string}
    config content-disarm
      Description: AV Content Disarm and Reconstruction settings.
      set analytics-suspicious [disable|enable]
      set cover-page [disable|enable]
      set detect-only [disable|enable]
      set error-action [block|log-only|...]
      set office-action [disable|enable]
      set office-dde [disable|enable]
      set office-embed [disable|enable]
      set office-hylink [disable|enable]
      set office-linked [disable|enable]
      set office-macro [disable|enable]
      set original-file-destination [fortisandbox|quarantine|...]
      set pdf-act-form [disable|enable]
      set pdf-act-gotor [disable|enable]
      set pdf-act-java [disable|enable]
  
```

```

    set pdf-act-launch [disable|enable]
    set pdf-act-movie [disable|enable]
    set pdf-act-sound [disable|enable]
    set pdf-embedfile [disable|enable]
    set pdf-hyperlink [disable|enable]
    set pdf-javacode [disable|enable]
end
set ems-threat-feed [disable|enable]
set extended-log [enable|disable]
set external-blocklist <name1>, <name2>, ...
set external-blocklist-enable-all [disable|enable]
set feature-set [flow|proxy]
set fortindr-error-action [log-only|block|...]
set fortindr-timeout-action [log-only|block|...]
set fortisandbox-error-action [log-only|block|...]
set fortisandbox-max-upload {integer}
set fortisandbox-mode [inline|analytics-suspicious|...]
set fortisandbox-timeout-action [log-only|block|...]
config ftp
    Description: Configure FTP AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set av-scan [disable|block|...]
    set emulator [enable|disable]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set malware-stream [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set quarantine [disable|enable]
end
config http
    Description: Configure HTTP AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set av-scan [disable|block|...]
    set content-disarm [disable|enable]
    set emulator [enable|disable]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set malware-stream [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set quarantine [disable|enable]
end
config imap
    Description: Configure IMAP AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set av-scan [disable|block|...]
    set content-disarm [disable|enable]
    set emulator [enable|disable]

```

```

    set executables [default|virus]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set malware-stream [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set quarantine [disable|enable]
end
config mapi
    Description: Configure MAPI AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set av-scan [disable|block|...]
    set emulator [enable|disable]
    set executables [default|virus]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set malware-stream [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set quarantine [disable|enable]
end
set mobile-malware-db [disable|enable]
config nac-quar
    Description: Configure AntiVirus quarantine settings.
    set expiry {user}
    set infected [none|quar-src-ip]
    set log [enable|disable]
end
config nntp
    Description: Configure NNTP AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set av-scan [disable|block|...]
    set emulator [enable|disable]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set malware-stream [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set quarantine [disable|enable]
end
set outbreak-prevention-archive-scan [disable|enable]
config pop3
    Description: Configure POP3 AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set av-scan [disable|block|...]
    set content-disarm [disable|enable]
    set emulator [enable|disable]
    set executables [default|virus]
    set external-blocklist [disable|block|...]

```

```

        set fortindr [disable|block|...]
        set fortisandbox [disable|block|...]
        set malware-stream [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set quarantine [disable|enable]
    end
    set replacemsg-group {string}
    set scan-mode [default|legacy]
    config smtp
        Description: Configure SMTP AntiVirus options.
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set av-scan [disable|block|...]
        set content-disarm [disable|enable]
        set emulator [enable|disable]
        set executables [default|virus]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set fortisandbox [disable|block|...]
        set malware-stream [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set quarantine [disable|enable]
    end
    config ssh
        Description: Configure SFTP and SCP AntiVirus options.
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set av-scan [disable|block|...]
        set emulator [enable|disable]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set fortisandbox [disable|block|...]
        set malware-stream [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set quarantine [disable|enable]
    end
next
end

```

config antivirus profile

Parameter	Description	Type	Size	Default
analytics-accept-filetype	Only submit files matching this DLP file-pattern to FortiSandbox (post-transfer scan only).	integer	Minimum value: 0 Maximum value: 4294967295	0
analytics-db	Enable/disable using the FortiSandbox signature database to supplement the AV signature databases.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Use only the standard AV signature databases.		
	<i>enable</i>	Also use the FortiSandbox signature database.		
analytics-ignore-filetype	Do not submit files matching this DLP file-pattern to FortiSandbox (post-transfer scan only).	integer	Minimum value: 0 Maximum value: 4294967295	
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
comment	Comment.	var-string	Maximum length: 255	
ems-threat-feed	Enable/disable use of EMS threat feed when performing AntiVirus scan. Analyzes files including the content of archives.	option	-	disable
	Option Description			
	<i>disable</i>	Disable use of EMS threat feed when performing AntiVirus scan.		
	<i>enable</i>	Enable use of EMS threat feed when performing AntiVirus scan.		
extended-log	Enable/disable extended logging for antivirus.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
external-blocklist <name>	One or more external malware block lists. External blocklist.	string	Maximum length: 79	
external-blocklist-enable-all	Enable/disable all external blocklists.	option	-	disable
	Option Description			
	<i>disable</i>	Use configured external blocklists.		
	<i>enable</i>	Enable all external blocklists.		

Parameter	Description	Type	Size	Default								
feature-set	Flow/proxy feature set.	option	-	flow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>flow</td><td>Flow feature set.</td></tr><tr><td>proxy</td><td>Proxy feature set.</td></tr></table>	Option	Description	flow	Flow feature set.	proxy	Proxy feature set.					
Option	Description											
flow	Flow feature set.											
proxy	Proxy feature set.											
fortindr-error-action *	Action to take if FortiNDR encounters an error.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log-only</td><td>Log FortiNDR error, but allow the file.</td></tr><tr><td>block</td><td>Block the file on FortiNDR error.</td></tr><tr><td>ignore</td><td>Do nothing on FortiNDR error.</td></tr></table>	Option	Description	log-only	Log FortiNDR error, but allow the file.	block	Block the file on FortiNDR error.	ignore	Do nothing on FortiNDR error.			
Option	Description											
log-only	Log FortiNDR error, but allow the file.											
block	Block the file on FortiNDR error.											
ignore	Do nothing on FortiNDR error.											
fortindr-timeout-action *	Action to take if FortiNDR encounters a scan timeout.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log-only</td><td>Log FortiNDR scan timeout, but allow the file.</td></tr><tr><td>block</td><td>Block the file on FortiNDR scan timeout.</td></tr><tr><td>ignore</td><td>Do nothing on FortiNDR scan timeout.</td></tr></table>	Option	Description	log-only	Log FortiNDR scan timeout, but allow the file.	block	Block the file on FortiNDR scan timeout.	ignore	Do nothing on FortiNDR scan timeout.			
Option	Description											
log-only	Log FortiNDR scan timeout, but allow the file.											
block	Block the file on FortiNDR scan timeout.											
ignore	Do nothing on FortiNDR scan timeout.											
fortisandbox-error-action *	Action to take if FortiSandbox inline scan encounters an error.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log-only</td><td>Log FortiSandbox inline scan error, but allow the file.</td></tr><tr><td>block</td><td>Block the file on FortiSandbox inline scan error.</td></tr><tr><td>ignore</td><td>Do nothing on FortiSandbox inline scan error.</td></tr></table>	Option	Description	log-only	Log FortiSandbox inline scan error, but allow the file.	block	Block the file on FortiSandbox inline scan error.	ignore	Do nothing on FortiSandbox inline scan error.			
Option	Description											
log-only	Log FortiSandbox inline scan error, but allow the file.											
block	Block the file on FortiSandbox inline scan error.											
ignore	Do nothing on FortiSandbox inline scan error.											
fortisandbox-max-upload	Maximum size of files that can be uploaded to FortiSandbox in Mbytes.	integer	Minimum value: 10 1 Maximum value: 1606 **									
fortisandbox-mode	FortiSandbox scan modes.	option	-	analytics-everything								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>inline</td><td>FortiSandbox inline scan.</td></tr></table>	Option	Description	inline	FortiSandbox inline scan.							
Option	Description											
inline	FortiSandbox inline scan.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>analytics-suspicious</i>	FortiSandbox post-transfer scan: submit supported files if heuristics or other methods determine they are suspicious.		
	<i>analytics-everything</i>	FortiSandbox post-transfer scan: submit supported files for inspection.		
fortisandbox-timeout-action *	Action to take if FortiSandbox inline scan encounters a scan timeout.	option	-	log-only
	Option	Description		
	<i>log-only</i>	Log FortiSandbox inline scan timeout, but allow the file.		
	<i>block</i>	Block the file on FortiSandbox inline scan timeout.		
	<i>ignore</i>	Do nothing on FortiSandbox inline scan timeout.		
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-	enable
	Option	Description		
	<i>disable</i>	Do not use the mobile malware signature database.		
	<i>enable</i>	Also use the mobile malware signature database.		
name	Profile name.	string	Maximum length: 47	
outbreak-prevention-archive-scan	Enable/disable outbreak-prevention archive scanning.	option	-	enable
	Option	Description		
	<i>disable</i>	Analyze files as sent, not the content of archives.		
	<i>enable</i>	Analyze files including the content of archives.		
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35	
scan-mode	Configure scan mode (default or legacy).	option	-	default
	Option	Description		
	<i>default</i>	On the fly decompression and scanning of certain archive files.		
	<i>legacy</i>	Scan archive files only after the entire file is received.		

* This parameter may not exist in some models.

** Values may differ between models.

config cifs

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	Option	Description		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS cannot open.		
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
emulator	Enable/disable the virus emulator.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		

* This parameter may not exist in some models.

config content-disarm

Parameter	Description	Type	Size	Default
analytics-suspicious	Enable/disable using CDR as a secondary method for determining suspicious files for analytics.	option	-	enable **
	Option	Description		
	<i>disable</i>			
	<i>enable</i>			
cover-page	Enable/disable inserting a cover page into the disarmed document.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
detect-only	Enable/disable only detect disarmable files, do not alter content.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
error-action	Action to be taken if CDR engine encounters an unrecoverable error.	option	-	log-only

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block file on CDR error.		
	<i>log-only</i>	Log CDR error, but allow file.		
	<i>ignore</i>	Do nothing on CDR error.		
office-action	Enable/disable stripping of PowerPoint action events in Microsoft Office documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-dde	Enable/disable stripping of Dynamic Data Exchange events in Microsoft Office documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-embed	Enable/disable stripping of embedded objects in Microsoft Office documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-hylink	Enable/disable stripping of hyperlinks in Microsoft Office documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-linked	Enable/disable stripping of linked objects in Microsoft Office documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		

Parameter	Description	Type	Size	Default								
office-macro	Enable/disable stripping of macros in Microsoft Office documents.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td>enable</td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	disable	Disable this Content Disarm and Reconstruction feature.	enable	Enable this Content Disarm and Reconstruction feature.					
Option	Description											
disable	Disable this Content Disarm and Reconstruction feature.											
enable	Enable this Content Disarm and Reconstruction feature.											
original-file-destination	Destination to send original file if active content is removed.	option	-	discard								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fortisandbox</td><td>Send original file to configured FortiSandbox.</td></tr><tr><td>quarantine</td><td>Send original file to quarantine.</td></tr><tr><td>discard</td><td>Original file will be discarded after content disarm.</td></tr></table>	Option	Description	fortisandbox	Send original file to configured FortiSandbox.	quarantine	Send original file to quarantine.	discard	Original file will be discarded after content disarm.			
Option	Description											
fortisandbox	Send original file to configured FortiSandbox.											
quarantine	Send original file to quarantine.											
discard	Original file will be discarded after content disarm.											
pdf-act-form	Enable/disable stripping of PDF document actions that submit data to other targets.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td>enable</td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	disable	Disable this Content Disarm and Reconstruction feature.	enable	Enable this Content Disarm and Reconstruction feature.					
Option	Description											
disable	Disable this Content Disarm and Reconstruction feature.											
enable	Enable this Content Disarm and Reconstruction feature.											
pdf-act-gotor	Enable/disable stripping of PDF document actions that access other PDF documents.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td>enable</td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	disable	Disable this Content Disarm and Reconstruction feature.	enable	Enable this Content Disarm and Reconstruction feature.					
Option	Description											
disable	Disable this Content Disarm and Reconstruction feature.											
enable	Enable this Content Disarm and Reconstruction feature.											
pdf-act-java	Enable/disable stripping of PDF document actions that execute JavaScript code.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td>enable</td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	disable	Disable this Content Disarm and Reconstruction feature.	enable	Enable this Content Disarm and Reconstruction feature.					
Option	Description											
disable	Disable this Content Disarm and Reconstruction feature.											
enable	Enable this Content Disarm and Reconstruction feature.											
pdf-act-launch	Enable/disable stripping of PDF document actions that launch other applications.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-sound	Enable/disable stripping of PDF document actions that play a sound.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-embedfile	Enable/disable stripping of embedded files in PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-hyperlink	Enable/disable stripping of hyperlinks from PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-javacode	Enable/disable stripping of JavaScript code in PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		

** Values may differ between models.

config ftp

Parameter	Description	Type	Size	Default																		
archive-block	Select the archive types to block.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Block encrypted archives.																					
<i>corrupted</i>	Block corrupted archives.																					
<i>partiallycorrupted</i>	Block partially corrupted archives.																					
<i>multipart</i>	Block multipart archives.																					
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Block mail bomb archives.																					
<i>timeout</i>	Block scan timeout.																					
<i>unhandled</i>	Block archives that FortiOS cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Log encrypted archives.																					
<i>corrupted</i>	Log corrupted archives.																					
<i>partiallycorrupted</i>	Log partially corrupted archives.																					
<i>multipart</i>	Log multipart archives.																					
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Log mail bomb archives.																					
<i>timeout</i>	Log scan timeout.																					
<i>unhandled</i>	Log archives that FortiOS cannot open.																					
av-scan	Enable AntiVirus scan service.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the virus infected files.</td></tr><tr><td><i>monitor</i></td><td>Log the virus infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.													
Option	Description																					
<i>disable</i>	Disable.																					
<i>block</i>	Block the virus infected files.																					
<i>monitor</i>	Log the virus infected files.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		

* This parameter may not exist in some models.

config http

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	Option	Description		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
	Option	Description												
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.												
	<i>mailbomb</i>	Log mail bomb archives.												
	<i>timeout</i>	Log scan timeout.												
<i>unhandled</i>	Log archives that FortiOS cannot open.													
av-scan	Enable AntiVirus scan service.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the virus infected files.</td></tr><tr><td><i>monitor</i></td><td>Log the virus infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.					
	Option	Description												
	<i>disable</i>	Disable.												
	<i>block</i>	Block the virus infected files.												
<i>monitor</i>	Log the virus infected files.													
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr><tr><td><i>enable</i></td><td>Enable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr></table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.							
	Option	Description												
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.												
<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.													
emulator	Enable/disable the virus emulator.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.							
	Option	Description												
	<i>enable</i>	Enable the virus emulator.												
<i>disable</i>	Disable the virus emulator.													
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.					
	Option	Description												
	<i>disable</i>	Disable.												
	<i>block</i>	Block the matched files.												
<i>monitor</i>	Log the matched files.													
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		

* This parameter may not exist in some models.

config imap

Parameter	Description	Type	Size	Default																		
archive-block	Select the archive types to block.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Block encrypted archives.																					
<i>corrupted</i>	Block corrupted archives.																					
<i>partiallycorrupted</i>	Block partially corrupted archives.																					
<i>multipart</i>	Block multipart archives.																					
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Block mail bomb archives.																					
<i>timeout</i>	Block scan timeout.																					
<i>unhandled</i>	Block archives that FortiOS cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Log encrypted archives.																					
<i>corrupted</i>	Log corrupted archives.																					
<i>partiallycorrupted</i>	Log partially corrupted archives.																					
<i>multipart</i>	Log multipart archives.																					
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Log mail bomb archives.																					
<i>timeout</i>	Log scan timeout.																					
<i>unhandled</i>	Log archives that FortiOS cannot open.																					
av-scan	Enable AntiVirus scan service.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the virus infected files.</td></tr><tr><td><i>monitor</i></td><td>Log the virus infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.													
Option	Description																					
<i>disable</i>	Disable.																					
<i>block</i>	Block the virus infected files.																					
<i>monitor</i>	Log the virus infected files.																					
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable																		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.		
	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.		
emulator	Enable/disable the virus emulator.	option	-	enable
	Option Description			
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option Description			
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.		
	<i>virus</i>	Treat Windows executables as viruses.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		

* This parameter may not exist in some models.

config mapi

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	Option	Description		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS cannot open.		
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
emulator	Enable/disable the virus emulator.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option	Description		
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.		
	<i>virus</i>	Treat Windows executables as viruses.		

Parameter	Description	Type	Size	Default								
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the matched files.											
<i>monitor</i>	Log the matched files.											
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiNDR detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiNDR detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiNDR detected infections.	<i>monitor</i>	Log the FortiNDR detected infections.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the FortiNDR detected infections.											
<i>monitor</i>	Log the FortiNDR detected infections.											
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiSandbox detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiSandbox detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiSandbox detected infections.	<i>monitor</i>	Log the FortiSandbox detected infections.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the FortiSandbox detected infections.											
<i>monitor</i>	Log the FortiSandbox detected infections.											
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the matched files.											
<i>monitor</i>	Log the matched files.											
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the matched files.											
<i>monitor</i>	Log the matched files.											
quarantine	Enable/disable quarantine for infected files.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		

* This parameter may not exist in some models.

config nac-quar

Parameter	Description	Type	Size	Default
expiry	Duration of quarantine.	user	Not Specified	5m
infected	Enable/Disable quarantining infected hosts to the banned user list.	option	-	none
	Option	Description		
	<i>none</i>	Do not quarantine infected hosts.		
	<i>quar-src-ip</i>	Quarantine all traffic from the infected hosts source IP.		
log	Enable/disable AntiVirus quarantine logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable AntiVirus quarantine logging.		
	<i>disable</i>	Disable AntiVirus quarantine logging.		

config nntp

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	Option	Description		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
av-scan	<i>unhandled</i>	Log archives that FortiOS cannot open.		
	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
emulator	<i>monitor</i>	Log the virus infected files.		
	Enable/disable the virus emulator.	option	-	enable
	Option	Description		
external-blocklist	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		

Parameter	Description	Type	Size	Default								
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>block</td><td>Block the FortiNDR detected infections.</td></tr><tr><td>monitor</td><td>Log the FortiNDR detected infections.</td></tr></table>	Option	Description	disable	Disable.	block	Block the FortiNDR detected infections.	monitor	Log the FortiNDR detected infections.			
Option	Description											
disable	Disable.											
block	Block the FortiNDR detected infections.											
monitor	Log the FortiNDR detected infections.											
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>block</td><td>Block the FortiSandbox detected infections.</td></tr><tr><td>monitor</td><td>Log the FortiSandbox detected infections.</td></tr></table>	Option	Description	disable	Disable.	block	Block the FortiSandbox detected infections.	monitor	Log the FortiSandbox detected infections.			
Option	Description											
disable	Disable.											
block	Block the FortiSandbox detected infections.											
monitor	Log the FortiSandbox detected infections.											
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>block</td><td>Block the matched files.</td></tr><tr><td>monitor</td><td>Log the matched files.</td></tr></table>	Option	Description	disable	Disable.	block	Block the matched files.	monitor	Log the matched files.			
Option	Description											
disable	Disable.											
block	Block the matched files.											
monitor	Log the matched files.											
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>block</td><td>Block the matched files.</td></tr><tr><td>monitor</td><td>Log the matched files.</td></tr></table>	Option	Description	disable	Disable.	block	Block the matched files.	monitor	Log the matched files.			
Option	Description											
disable	Disable.											
block	Block the matched files.											
monitor	Log the matched files.											
quarantine	Enable/disable quarantine for infected files.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable quarantine for infected files.</td></tr><tr><td>enable</td><td>Enable quarantine for infected files.</td></tr></table>	Option	Description	disable	Disable quarantine for infected files.	enable	Enable quarantine for infected files.					
Option	Description											
disable	Disable quarantine for infected files.											
enable	Enable quarantine for infected files.											

* This parameter may not exist in some models.

config pop3

Parameter	Description	Type	Size	Default																		
archive-block	Select the archive types to block.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Block encrypted archives.																					
<i>corrupted</i>	Block corrupted archives.																					
<i>partiallycorrupted</i>	Block partially corrupted archives.																					
<i>multipart</i>	Block multipart archives.																					
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Block mail bomb archives.																					
<i>timeout</i>	Block scan timeout.																					
<i>unhandled</i>	Block archives that FortiOS cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Log encrypted archives.																					
<i>corrupted</i>	Log corrupted archives.																					
<i>partiallycorrupted</i>	Log partially corrupted archives.																					
<i>multipart</i>	Log multipart archives.																					
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Log mail bomb archives.																					
<i>timeout</i>	Log scan timeout.																					
<i>unhandled</i>	Log archives that FortiOS cannot open.																					
av-scan	Enable AntiVirus scan service.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the virus infected files.</td></tr><tr><td><i>monitor</i></td><td>Log the virus infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.													
Option	Description																					
<i>disable</i>	Disable.																					
<i>block</i>	Block the virus infected files.																					
<i>monitor</i>	Log the virus infected files.																					
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable																		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.		
	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.		
emulator	Enable/disable the virus emulator.	option	-	enable
	Option Description			
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option Description			
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.		
	<i>virus</i>	Treat Windows executables as viruses.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		

* This parameter may not exist in some models.

config smtp

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.													
	Option	Description																				
	<i>mailbomb</i>	Block mail bomb archives.																				
	<i>timeout</i>	Block scan timeout.																				
<i>unhandled</i>	Block archives that FortiOS cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
	Option	Description																				
	<i>encrypted</i>	Log encrypted archives.																				
	<i>corrupted</i>	Log corrupted archives.																				
	<i>partiallycorrupted</i>	Log partially corrupted archives.																				
	<i>multipart</i>	Log multipart archives.																				
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Log mail bomb archives.																				
	<i>timeout</i>	Log scan timeout.																				
<i>unhandled</i>	Log archives that FortiOS cannot open.																					
av-scan	Enable AntiVirus scan service.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the virus infected files.</td></tr><tr><td><i>monitor</i></td><td>Log the virus infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.													
	Option	Description																				
	<i>disable</i>	Disable.																				
	<i>block</i>	Block the virus infected files.																				
<i>monitor</i>	Log the virus infected files.																					
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr><tr><td><i>enable</i></td><td>Enable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr></table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.															
	Option	Description																				
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.																				
<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.																	
	Option	Description																				
<i>enable</i>	Enable the virus emulator.																					

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>disable</i>	Disable the virus emulator.							
	Option	Description										
	<i>disable</i>	Disable the virus emulator.										
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td><i>virus</i></td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.					
	Option	Description										
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.										
<i>virus</i>	Treat Windows executables as viruses.											
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the matched files.										
<i>monitor</i>	Log the matched files.											
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiNDR detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiNDR detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiNDR detected infections.	<i>monitor</i>	Log the FortiNDR detected infections.			
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the FortiNDR detected infections.										
<i>monitor</i>	Log the FortiNDR detected infections.											
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiSandbox detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiSandbox detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiSandbox detected infections.	<i>monitor</i>	Log the FortiSandbox detected infections.			
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the FortiSandbox detected infections.										
<i>monitor</i>	Log the FortiSandbox detected infections.											
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the matched files.										
<i>monitor</i>	Log the matched files.											

Parameter	Description	Type	Size	Default								
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the matched files.											
<i>monitor</i>	Log the matched files.											
quarantine	Enable/disable quarantine for infected files.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine for infected files.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine for infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine for infected files.	<i>enable</i>	Enable quarantine for infected files.					
Option	Description											
<i>disable</i>	Disable quarantine for infected files.											
<i>enable</i>	Enable quarantine for infected files.											

* This parameter may not exist in some models.

config ssh

Parameter	Description	Type	Size	Default																		
archive-block	Select the archive types to block.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Block encrypted archives.																					
<i>corrupted</i>	Block corrupted archives.																					
<i>partiallycorrupted</i>	Block partially corrupted archives.																					
<i>multipart</i>	Block multipart archives.																					
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Block mail bomb archives.																					
<i>timeout</i>	Block scan timeout.																					
<i>unhandled</i>	Block archives that FortiOS cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.													
Option	Description																					
<i>encrypted</i>	Log encrypted archives.																					
<i>corrupted</i>	Log corrupted archives.																					
<i>partiallycorrupted</i>	Log partially corrupted archives.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS cannot open.		
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
emulator	Enable/disable the virus emulator.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr *	Enable scanning of files by FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
malware-stream	Enable 0-day malware-stream scanning. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		

* This parameter may not exist in some models.

config antivirus quarantine

Configure quarantine options.

```
config antivirus quarantine
  Description: Configure quarantine options.
  set agelimit {integer}
  set destination [NULL|disk|...]
  set drop-infected {option1}, {option2}, ...
  set drop-machine-learning {option1}, {option2}, ...
  set lowspace [drop-new|ovrw-old]
  set maxfilesize {integer}
```

```

set quarantine-quota {integer}
set store-infected {option1}, {option2}, ...
set store-machine-learning {option1}, {option2}, ...
end

```

config antivirus quarantine

Parameter	Description	Type	Size	Default
agelimit	Age limit for quarantined files (0 - 479 hours, 0 means forever).	integer	Minimum value: 0 Maximum value: 479	0
destination	Choose whether to quarantine files to the FortiGate disk or to FortiAnalyzer or to delete them instead of quarantining them.	option	-	disk **
	Option		Description	
	NULL		Files that would be quarantined are deleted.	
	disk		Quarantine files to the FortiGate hard disk.	
	FortiAnalyzer		FortiAnalyzer	
drop-infected	Do not quarantine infected files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-	
	Option		Description	
	imap		IMAP.	
	smtp		SMTP.	
	pop3		POP3.	
	http		HTTP.	
	ftp		FTP.	
	nntp		NNTP.	
	imaps		IMAPS.	
	smtps		SMTPS.	
	pop3s		POP3S.	
	https		HTTPS.	
	ftps		FTPS.	
	mapi		MAPI.	
	cifs		CIFS.	

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssh</td><td>SSH.</td></tr></table>	Option	Description	ssh	SSH.																													
	Option	Description																																
ssh	SSH.																																	
drop-machine-learning	Do not quarantine files detected by machine learning found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>imap</td><td>IMAP.</td></tr><tr><td>smtp</td><td>SMTP.</td></tr><tr><td>pop3</td><td>POP3.</td></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>nntp</td><td>NNTP.</td></tr><tr><td>imaps</td><td>IMAPS.</td></tr><tr><td>smtps</td><td>SMTPS.</td></tr><tr><td>pop3s</td><td>POP3S.</td></tr><tr><td>https</td><td>HTTPS.</td></tr><tr><td>ftps</td><td>FTPS.</td></tr><tr><td>mapi</td><td>MAPI.</td></tr><tr><td>cifs</td><td>CIFS.</td></tr><tr><td>ssh</td><td>SSH.</td></tr></table>	Option	Description	imap	IMAP.	smtp	SMTP.	pop3	POP3.	http	HTTP.	ftp	FTP.	nntp	NNTP.	imaps	IMAPS.	smtps	SMTPS.	pop3s	POP3S.	https	HTTPS.	ftps	FTPS.	mapi	MAPI.	cifs	CIFS.	ssh	SSH.			
	Option	Description																																
	imap	IMAP.																																
	smtp	SMTP.																																
	pop3	POP3.																																
	http	HTTP.																																
	ftp	FTP.																																
	nntp	NNTP.																																
	imaps	IMAPS.																																
	smtps	SMTPS.																																
	pop3s	POP3S.																																
	https	HTTPS.																																
	ftps	FTPS.																																
	mapi	MAPI.																																
cifs	CIFS.																																	
ssh	SSH.																																	
lowspace	Select the method for handling additional files when running low on disk space.	option	-	ovrw-old																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop-new</td><td>Drop (delete) the most recently quarantined files.</td></tr><tr><td>ovrw-old</td><td>Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.</td></tr></table>	Option	Description	drop-new	Drop (delete) the most recently quarantined files.	ovrw-old	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.																											
	Option	Description																																
	drop-new	Drop (delete) the most recently quarantined files.																																
ovrw-old	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.																																	
maxfilesize	Maximum file size to quarantine (0 - 500 Mbytes, 0 means unlimited).	integer	Minimum value: 0 0 Maximum value: 500																															

Parameter	Description	Type	Size	Default
quarantine-quota	The amount of disk space to reserve for quarantining files (0 - 4294967295 Mbytes, 0 means unlimited and depends on disk space).	integer	Minimum value: 0 Maximum value: 4294967295	0
store-infected	Quarantine infected files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh

Option	Description
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>http</i>	HTTP.
<i>ftp</i>	FTP.
<i>nntp</i>	NNTP.
<i>imaps</i>	IMAPS.
<i>smtps</i>	SMTPS.
<i>pop3s</i>	POP3S.
<i>https</i>	HTTPS.
<i>ftps</i>	FTPS.
<i>mapi</i>	MAPI.
<i>cifs</i>	CIFS.
<i>ssh</i>	SSH.

Parameter	Description	Type	Size	Default
store-machine-learning	Quarantine files detected by machine learning found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh

Option	Description
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>http</i>	HTTP.
<i>ftp</i>	FTP.
<i>nntp</i>	NNTP.
<i>imaps</i>	IMAPS.
<i>smtps</i>	SMTPS.
<i>pop3s</i>	POP3S.
<i>https</i>	HTTPS.
<i>ftps</i>	FTPS.
<i>mapi</i>	MAPI.
<i>cifs</i>	CIFS.
<i>ssh</i>	SSH.

** Values may differ between models.

config antivirus settings

Configure AntiVirus settings.

```
config antivirus settings
  Description: Configure AntiVirus settings.
  set cache-infected-result [enable|disable]
  set grayware [enable|disable]
  set machine-learning-detection [enable|monitor|...]
  set override-timeout {integer}
```

```

set use-extreme-db [enable|disable]
end

```

config antivirus settings

Parameter	Description	Type	Size	Default
cache-infected-result	Enable/disable cache of infected scan results (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable cache of infected scan results.		
	<i>disable</i>	Disable cache of infected scan results.		
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable grayware detection.		
	<i>disable</i>	Disable grayware detection.		
machine-learning-detection	Use machine learning based malware detection.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable machine learning based malware detection.		
	<i>monitor</i>	Enable machine learning based malware detection for monitoring only.		
	<i>disable</i>	Disable machine learning based malware detection.		
override-timeout	Override the large file scan timeout value in seconds (30 - 3600). Zero is the default value and is used to disable this command. When disabled, the daemon adjusts the large file scan timeout based on the file size.	integer	Minimum value: 30 Maximum value: 3600	0
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable extreme AVDB.		
	<i>disable</i>	Disable extreme AVDB.		

application

This section includes syntax for the following commands:

- [config application custom on page 161](#)
- [config application group on page 162](#)
- [config application list on page 163](#)
- [config application name on page 172](#)
- [config application rule-settings on page 174](#)

config application custom

Configure custom application signatures.

```
config application custom
  Description: Configure custom application signatures.
  edit <tag>
    set behavior {user}
    set category {integer}
    set comment {string}
    set id {integer}
    set protocol {user}
    set signature {var-string}
    set technology {user}
    set vendor {user}
  next
end
```

config application custom

Parameter	Description	Type	Size	Default
behavior	Custom application signature behavior.	user	Not Specified	
category	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	
comment	Comment.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
id	Custom application category ID (use ? to view available options). Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Custom application signature protocol.	user	Not Specified	
signature	The text that makes up the actual custom application signature.	var-string	Maximum length: 4095	
tag	Signature tag.	string	Maximum length: 63	
technology	Custom application signature technology.	user	Not Specified	
vendor	Custom application signature vendor.	user	Not Specified	

config application group

Configure firewall application groups.

```
config application group
  Description: Configure firewall application groups.
  edit <name>
    set application <id1>, <id2>, ...
    set behavior {user}
    set category <id1>, <id2>, ...
    set comment {var-string}
    set popularity {option1}, {option2}, ...
    set protocols {user}
    set risk <level1>, <level2>, ...
    set technology {user}
    set type [application|filter]
    set vendor {user}
  next
end
```

config application group

Parameter	Description	Type	Size	Default
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
behavior	Application behavior filter.	user	Not Specified	all

Parameter	Description	Type	Size	Default												
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
comment	Comments.	var-string	Maximum length: 255													
name	Application group name.	string	Maximum length: 63													
popularity	Application popularity filter (1 - 5, from least to most popular).	option	-	1 2 3 4 5												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Popularity level 1.</td></tr><tr><td>2</td><td>Popularity level 2.</td></tr><tr><td>3</td><td>Popularity level 3.</td></tr><tr><td>4</td><td>Popularity level 4.</td></tr><tr><td>5</td><td>Popularity level 5.</td></tr></table>				Option	Description	1	Popularity level 1.	2	Popularity level 2.	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.
Option	Description															
1	Popularity level 1.															
2	Popularity level 2.															
3	Popularity level 3.															
4	Popularity level 4.															
5	Popularity level 5.															
protocols	Application protocol filter.	user	Not Specified	all												
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295													
technology	Application technology filter.	user	Not Specified	all												
type	Application group type.	option	-	application												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>application</td><td>Application ID.</td></tr><tr><td>filter</td><td>Application filter.</td></tr></table>				Option	Description	application	Application ID.	filter	Application filter.						
Option	Description															
application	Application ID.															
filter	Application filter.															
vendor	Application vendor filter.	user	Not Specified	all												

config application list

Configure application control lists.

```

config application list
    Description: Configure application control lists.
    edit <name>
        set app-replacemsg [disable|enable]
        set comment {var-string}
        set control-default-network-services [disable|enable]
        set deep-app-inspection [disable|enable]
        config default-network-services
            Description: Default network service entries.
            edit <id>
                set port {integer}
                set services {option1}, {option2}, ...
                set violation-action [pass|monitor|...]
            next
        end
    set enforce-default-app-port [disable|enable]
    config entries
        Description: Application list entries.
        edit <id>
            set action [pass|block|...]
            set application <id1>, <id2>, ...
            set behavior {user}
            set category <id1>, <id2>, ...
            set exclusion <id1>, <id2>, ...
            set log [disable|enable]
            set log-packet [disable|enable]
            config parameters
                Description: Application parameters.
                edit <id>
                    config members
                        Description: Parameter tuple members.
                        edit <id>
                            set name {string}
                            set value {string}
                        next
                    end
                next
            end
        set per-ip-shaper {string}
        set popularity {option1}, {option2}, ...
        set protocols {user}
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set rate-count {integer}
        set rate-duration {integer}
        set rate-mode [periodical|continuous]
        set rate-track [none|src-ip|...]
        set risk <level1>, <level2>, ...
        set session-ttl {integer}
        set shaper {string}
        set shaper-reverse {string}

```

```

        set technology {user}
        set vendor {user}
    next
end
set extended-log [enable|disable]
set force-inclusion-ssl-di-sigs [disable|enable]
set options {option1}, {option2}, ...
set other-application-action [pass|block]
set other-application-log [disable|enable]
set p2p-block-list {option1}, {option2}, ...
set replacemsg-group {string}
set unknown-application-action [pass|block]
set unknown-application-log [disable|enable]
next
end

```

config application list

Parameter	Description	Type	Size	Default						
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable replacement messages for blocked applications.</td></tr><tr><td>enable</td><td>Enable replacement messages for blocked applications.</td></tr></table>	Option	Description	disable	Disable replacement messages for blocked applications.	enable	Enable replacement messages for blocked applications.			
Option	Description									
disable	Disable replacement messages for blocked applications.									
enable	Enable replacement messages for blocked applications.									
comment	Comments.	var-string	Maximum length: 255							
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable protocol enforcement over selected ports.</td></tr><tr><td>enable</td><td>Enable protocol enforcement over selected ports.</td></tr></table>	Option	Description	disable	Disable protocol enforcement over selected ports.	enable	Enable protocol enforcement over selected ports.			
Option	Description									
disable	Disable protocol enforcement over selected ports.									
enable	Enable protocol enforcement over selected ports.									
deep-app-inspection	Enable/disable deep application inspection.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable deep application inspection.</td></tr><tr><td>enable</td><td>Enable deep application inspection.</td></tr></table>	Option	Description	disable	Disable deep application inspection.	enable	Enable deep application inspection.			
Option	Description									
disable	Disable deep application inspection.									
enable	Enable deep application inspection.									

Parameter	Description	Type	Size	Default										
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable default application port enforcement.</td></tr><tr><td><i>enable</i></td><td>Enable default application port enforcement.</td></tr></table>	Option	Description	<i>disable</i>	Disable default application port enforcement.	<i>enable</i>	Enable default application port enforcement.							
Option	Description													
<i>disable</i>	Disable default application port enforcement.													
<i>enable</i>	Enable default application port enforcement.													
extended-log	Enable/disable extended logging.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
force-inclusion-ssl-di-sigs	Enable/disable forced inclusion of SSL deep inspection signatures.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable forced inclusion of signatures which normally require SSL deep inspection.</td></tr><tr><td><i>enable</i></td><td>Enable forced inclusion of signatures which normally require SSL deep inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.	<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.							
Option	Description													
<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.													
<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.													
name	List name.	string	Maximum length: 47											
options	Basic application protocol signatures allowed by default.	option	-	allow-dns										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow-dns</i></td><td>Allow DNS.</td></tr><tr><td><i>allow-icmp</i></td><td>Allow ICMP.</td></tr><tr><td><i>allow-http</i></td><td>Allow generic HTTP web browsing.</td></tr><tr><td><i>allow-ssl</i></td><td>Allow generic SSL communication.</td></tr></table>	Option	Description	<i>allow-dns</i>	Allow DNS.	<i>allow-icmp</i>	Allow ICMP.	<i>allow-http</i>	Allow generic HTTP web browsing.	<i>allow-ssl</i>	Allow generic SSL communication.			
Option	Description													
<i>allow-dns</i>	Allow DNS.													
<i>allow-icmp</i>	Allow ICMP.													
<i>allow-http</i>	Allow generic HTTP web browsing.													
<i>allow-ssl</i>	Allow generic SSL communication.													
other-application-action	Action for other applications.	option	-	pass										

Parameter	Description	Type	Size	Default
	Option Description			
	<i>pass</i>	Allow sessions matching an application in this application list.		
	<i>block</i>	Block sessions matching an application in this application list.		
other-application-log	Enable/disable logging for other applications.	option	-	disable
	Option Description			
	<i>disable</i>	Disable logging for other applications.		
	<i>enable</i>	Enable logging for other applications.		
p2p-block-list	P2P applications to be block listed.	option	-	
	Option Description			
	<i>skype</i>	Skype.		
	<i>edonkey</i>	Edonkey.		
	<i>bittorrent</i>	Bit torrent.		
replacemsg-group	Replacement message group.	string	Maximum length: 35	
unknown-application-action	Pass or block traffic from unknown applications.	option	-	pass
	Option Description			
	<i>pass</i>	Pass or allow unknown applications.		
	<i>block</i>	Drop or block unknown applications.		
unknown-application-log	Enable/disable logging for unknown applications.	option	-	disable
	Option Description			
	<i>disable</i>	Disable logging for unknown applications.		
	<i>enable</i>	Enable logging for unknown applications.		

config default-network-services

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
port	Port number.	integer	Minimum value: 0 0 Maximum value: 65535	0
services	Network protocols.	option	-	
	Option	Description		
	http	HTTP.		
	ssh	SSH.		
	telnet	TELNET.		
	ftp	FTP.		
	dns	DNS.		
	smtp	SMTP.		
	pop3	POP3.		
	imap	IMAP.		
	snmp	SNMP.		
	nntp	NNTP.		
	https	HTTPS.		
	violation-action	Action for protocols not in the allowlist for selected port.	option	-
	Option	Description		
	pass	Allow protocols not in the allowlist for selected port.		
	monitor	Monitor protocols not in the allowlist for selected port.		
	block	Block protocols not in the allowlist for selected port.		

config entries

Parameter	Description	Type	Size	Default
action	Pass or block traffic, or reset connection for traffic from this application.	option	-	block

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
behavior	Application behavior filter.	user	Not Specified	all
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
log	Enable/disable logging for this application list.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
log-packet	Enable/disable packet logging.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable packet logging.		
	<i>enable</i>	Enable packet logging.		
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35	
popularity	Application popularity filter (1 - 5, from least to most popular).	option	-	1 2 3 4 5

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Popularity level 1.</td></tr><tr><td>2</td><td>Popularity level 2.</td></tr><tr><td>3</td><td>Popularity level 3.</td></tr><tr><td>4</td><td>Popularity level 4.</td></tr><tr><td>5</td><td>Popularity level 5.</td></tr></table>	Option	Description	1	Popularity level 1.	2	Popularity level 2.	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.			
	Option	Description														
	1	Popularity level 1.														
	2	Popularity level 2.														
	3	Popularity level 3.														
	4	Popularity level 4.														
5	Popularity level 5.															
protocols	Application protocol filter.	user	Not Specified	all												
quarantine	Quarantine method.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Quarantine is disabled.</td></tr><tr><td>attacker</td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>	Option	Description	none	Quarantine is disabled.	attacker	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
	Option	Description														
	none	Quarantine is disabled.														
attacker	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.															
quarantine-expiry	Duration of quarantine. (Format ####d##h##m, minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified	5m												
quarantine-log	Enable/disable quarantine logging.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable quarantine logging.</td></tr><tr><td>enable</td><td>Enable quarantine logging.</td></tr></table>	Option	Description	disable	Disable quarantine logging.	enable	Enable quarantine logging.									
	Option	Description														
	disable	Disable quarantine logging.														
enable	Enable quarantine logging.															
rate-count	Count of the rate.	integer	Minimum value: 0 0 Maximum value: 65535													
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 60 1 Maximum value: 65535													
rate-mode	Rate limit mode.	option	-	continuous												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>periodical</td><td>Allow configured number of packets every rate-duration.</td></tr><tr><td>continuous</td><td>Block packets once the rate is reached.</td></tr></table>	Option	Description	periodical	Allow configured number of packets every rate-duration.	continuous	Block packets once the rate is reached.									
	Option	Description														
	periodical	Allow configured number of packets every rate-duration.														
continuous	Block packets once the rate is reached.															

Parameter	Description	Type	Size	Default
rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	none		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
	<i>dhcp-client-mac</i>	DHCP client.		
	<i>dns-domain</i>	DNS domain.		
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295	
session-ttl	Session TTL (0 = default).	integer	Minimum value: 0 Maximum value: 4294967295	
shaper	Traffic shaper.	string	Maximum length: 35	
shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35	
technology	Application technology filter.	user	Not Specified	all
vendor	Application vendor filter.	user	Not Specified	all

config parameters

Parameter	Description	Type	Size	Default
id	Parameter tuple ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config members

Parameter	Description	Type	Size	Default
id	Parameter.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

config application name

Configure application signatures. Read-only.

```
config application name
  Description: Configure application signatures. Read-only.
  edit <name>
    set behavior {user}
    set category {integer}
    set id {integer}
    config metadata
      Description: Meta data. Read-only.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
  config parameters
    Description: Application parameters. Read-only.
    edit <name>
      set default value {string}
    next
  end
  set popularity {integer}
  set protocol {user}
  set risk {integer}
  set technology {user}
  set vendor {user}
  set weight {integer}
next
end
```

config application name

Parameter	Description	Type	Size	Default
behavior	Application behavior. Read-only.	user	Not Specified	
category	Application category ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
id	Application ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
name	Application name.	string	Maximum length: 63	
popularity	Application popularity. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	
protocol	Application protocol. Read-only.	user	Not Specified	
risk	Application risk. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	
technology	Application technology. Read-only.	user	Not Specified	
vendor	Application vendor. Read-only.	user	Not Specified	
weight	Application weight. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	

config metadata

Parameter	Description	Type	Size	Default
id	ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
metaid	Meta ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
valueid	Value ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

config parameters

Parameter	Description	Type	Size	Default
default value	Parameter default value. Read-only.	string	Maximum length: 199	
name	Parameter name. Read-only.	string	Maximum length: 31	

config application rule-settings

Configure application rule settings. Read-only.

```
config application rule-settings
    Description: Configure application rule settings. Read-only.
    edit <id>
        next
    end
```

config application rule-settings

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

authentication

This section includes syntax for the following commands:

- [config authentication rule on page 175](#)
- [config authentication scheme on page 178](#)
- [config authentication setting on page 180](#)

config authentication rule

Configure Authentication Rules.

```
config authentication rule
  Description: Configure Authentication Rules.
  edit <name>
    set active-auth-method {string}
    set cert-auth-cookie [enable|disable]
    set comments {var-string}
    set cors-depth {integer}
    set cors-stateful [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set ip-based [enable|disable]
    set protocol [http|ftp|...]
    set srcaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set srcintf <name1>, <name2>, ...
    set sso-auth-method {string}
    set status [enable|disable]
    set transaction-based [enable|disable]
    set web-auth-cookie [enable|disable]
    set web-portal [enable|disable]
  next
end
```

config authentication rule

Parameter	Description	Type	Size	Default
active-auth-method	Select an active authentication method.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
cert-auth-cookie	Enable/disable to use device certificate as authentication cookie (default = enable).	option	-	enable
	Option	Description		
	enable	Enable device certificate as authentication cookie.		
	disable	Disable device certificate as authentication cookie.		
comments	Comment.	var-string	Maximum length: 1023	
cors-depth	Depth to allow CORS access (default = 3).	integer	Minimum value: 1 Maximum value: 8	3
cors-stateful	Enable/disable allowance of CORS access (default = disable).	option	-	disable
	Option	Description		
	enable	Enable allowance of CORS access		
	disable	Disable allowance of CORS access		
dstaddr <name>	Select an IPv4 destination address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79	
dstaddr6 <name>	Select an IPv6 destination address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79	
ip-based	Enable/disable IP-based authentication. When enabled, previously authenticated users from the same IP address will be exempted.	option	-	enable
	Option	Description		
	enable	Enable IP-based authentication.		
	disable	Disable IP-based authentication.		
name	Authentication rule name.	string	Maximum length: 35	
protocol	Authentication is required for the selected protocol (default = HTTP).	option	-	http

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP traffic is matched and authentication is required.</td></tr><tr><td>ftp</td><td>FTP traffic is matched and authentication is required.</td></tr><tr><td>socks</td><td>SOCKS traffic is matched and authentication is required.</td></tr><tr><td>ssh</td><td>SSH traffic is matched and authentication is required.</td></tr><tr><td>ztna-portal</td><td>ZTNA portal traffic is matched and authentication is required.</td></tr></table>	Option	Description	http	HTTP traffic is matched and authentication is required.	ftp	FTP traffic is matched and authentication is required.	socks	SOCKS traffic is matched and authentication is required.	ssh	SSH traffic is matched and authentication is required.	ztna-portal	ZTNA portal traffic is matched and authentication is required.			
Option	Description															
http	HTTP traffic is matched and authentication is required.															
ftp	FTP traffic is matched and authentication is required.															
socks	SOCKS traffic is matched and authentication is required.															
ssh	SSH traffic is matched and authentication is required.															
ztna-portal	ZTNA portal traffic is matched and authentication is required.															
srcaddr <name>	Authentication is required for the selected IPv4 source address. Address name.	string	Maximum length: 79													
srcaddr6 <name>	Authentication is required for the selected IPv6 source address. Address name.	string	Maximum length: 79													
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79													
sso-auth-method	Select a single-sign on (SSO) authentication method.	string	Maximum length: 35													
status	Enable/disable this authentication rule.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this authentication rule.</td></tr><tr><td>disable</td><td>Disable this authentication rule.</td></tr></table>	Option	Description	enable	Enable this authentication rule.	disable	Disable this authentication rule.									
Option	Description															
enable	Enable this authentication rule.															
disable	Disable this authentication rule.															
transaction-based	Enable/disable transaction based authentication (default = disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable transaction based authentication.</td></tr><tr><td>disable</td><td>Disable transaction based authentication.</td></tr></table>	Option	Description	enable	Enable transaction based authentication.	disable	Disable transaction based authentication.									
Option	Description															
enable	Enable transaction based authentication.															
disable	Disable transaction based authentication.															
web-auth-cookie	Enable/disable Web authentication cookies (default = disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Web authentication cookie.</td></tr><tr><td>disable</td><td>Disable Web authentication cookie.</td></tr></table>	Option	Description	enable	Enable Web authentication cookie.	disable	Disable Web authentication cookie.									
Option	Description															
enable	Enable Web authentication cookie.															
disable	Disable Web authentication cookie.															

Parameter	Description	Type	Size	Default
web-portal	Enable/disable web portal for proxy transparent policy (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable web-portal.		
	<i>disable</i>	Disable web-portal.		

config authentication scheme

Configure Authentication Schemes.

```

config authentication scheme
  Description: Configure Authentication Schemes.
  edit <name>
    set digest-algo {option1}, {option2}, ...
    set domain-controller {string}
    set external-idp {string}
    set fsso-agent-for-ntlm {string}
    set fsso-guest [enable|disable]
    set group-attr-type [display-name|external-id]
    set kerberos-keytab {string}
    set method {option1}, {option2}, ...
    set negotiate-ntlm [enable|disable]
    set require-tfa [enable|disable]
    set saml-server {string}
    set saml-timeout {integer}
    set ssh-ca {string}
    set user-cert [enable|disable]
    set user-database <name1>, <name2>, ...
  next
end

```

config authentication scheme

Parameter	Description	Type	Size	Default
digest-algo	Digest Authentication Algorithms.	option	-	md5 sha-256
	Option	Description		
	<i>md5</i>	MD5.		
	<i>sha-256</i>	SHA-256.		

Parameter	Description	Type	Size	Default																								
domain-controller	Domain controller setting.	string	Maximum length: 35																									
external-idp	External identity provider configuration.	string	Maximum length: 35																									
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35																									
fsso-guest	Enable/disable user fsso-guest authentication (default = disable).	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user fsso-guest authentication.</td></tr><tr><td><i>disable</i></td><td>Disable user fsso-guest authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable user fsso-guest authentication.	<i>disable</i>	Disable user fsso-guest authentication.																		
	Option	Description																										
	<i>enable</i>	Enable user fsso-guest authentication.																										
<i>disable</i>	Disable user fsso-guest authentication.																											
group-attr-type	Group attribute type used to match SCIM groups (default = display-name).	option	-	display-name																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>display-name</i></td><td>Display name.</td></tr><tr><td><i>external-id</i></td><td>External ID.</td></tr></table>				Option	Description	<i>display-name</i>	Display name.	<i>external-id</i>	External ID.																		
	Option	Description																										
	<i>display-name</i>	Display name.																										
<i>external-id</i>	External ID.																											
kerberos-keytab	Kerberos keytab setting.	string	Maximum length: 35																									
method	Authentication methods (default = basic).	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ntlm</i></td><td>NTLM authentication.</td></tr><tr><td><i>basic</i></td><td>Basic HTTP authentication.</td></tr><tr><td><i>digest</i></td><td>Digest HTTP authentication.</td></tr><tr><td><i>form</i></td><td>Form-based HTTP authentication.</td></tr><tr><td><i>negotiate</i></td><td>Negotiate authentication.</td></tr><tr><td><i>fsso</i></td><td>Fortinet Single Sign-On (FSSO) authentication.</td></tr><tr><td><i>rssso</i></td><td>RADIUS Single Sign-On (RSSO) authentication.</td></tr><tr><td><i>ssh-publickey</i></td><td>Public key based SSH authentication.</td></tr><tr><td><i>cert</i></td><td>Client certificate authentication.</td></tr><tr><td><i>saml</i></td><td>SAML authentication.</td></tr><tr><td><i>entra-ssso</i></td><td>Entra ID based Single Sign-On (SSO) authentication.</td></tr></table>				Option	Description	<i>ntlm</i>	NTLM authentication.	<i>basic</i>	Basic HTTP authentication.	<i>digest</i>	Digest HTTP authentication.	<i>form</i>	Form-based HTTP authentication.	<i>negotiate</i>	Negotiate authentication.	<i>fsso</i>	Fortinet Single Sign-On (FSSO) authentication.	<i>rssso</i>	RADIUS Single Sign-On (RSSO) authentication.	<i>ssh-publickey</i>	Public key based SSH authentication.	<i>cert</i>	Client certificate authentication.	<i>saml</i>	SAML authentication.	<i>entra-ssso</i>	Entra ID based Single Sign-On (SSO) authentication.
	Option	Description																										
	<i>ntlm</i>	NTLM authentication.																										
	<i>basic</i>	Basic HTTP authentication.																										
	<i>digest</i>	Digest HTTP authentication.																										
	<i>form</i>	Form-based HTTP authentication.																										
	<i>negotiate</i>	Negotiate authentication.																										
	<i>fsso</i>	Fortinet Single Sign-On (FSSO) authentication.																										
	<i>rssso</i>	RADIUS Single Sign-On (RSSO) authentication.																										
	<i>ssh-publickey</i>	Public key based SSH authentication.																										
	<i>cert</i>	Client certificate authentication.																										
	<i>saml</i>	SAML authentication.																										
<i>entra-ssso</i>	Entra ID based Single Sign-On (SSO) authentication.																											

Parameter	Description	Type	Size	Default
name	Authentication scheme name.	string	Maximum length: 35	
negotiate-ntlm	Enable/disable negotiate authentication for NTLM (default = disable).	option	-	enable
	Option	Description		
	enable	Enable negotiate authentication for NTLM.		
	disable	Disable negotiate authentication for NTLM.		
require-tfa	Enable/disable two-factor authentication (default = disable).	option	-	disable
	Option	Description		
	enable	Enable two-factor authentication.		
	disable	Disable two-factor authentication.		
saml-server	SAML configuration.	string	Maximum length: 35	
saml-timeout	SAML authentication timeout in seconds.	integer	Minimum value: 30 Maximum value: 1200	120
ssh-ca	SSH CA name.	string	Maximum length: 35	
user-cert	Enable/disable authentication with user certificate (default = disable).	option	-	disable
	Option	Description		
	enable	Enable client certificate field authentication.		
	disable	Disable client certificate field authentication.		
user-database <name>	Authentication server to contain user information; "local-user-db" (default) or "123" (for LDAP). Authentication server name.	string	Maximum length: 79	

config authentication setting

Configure authentication setting.

```
config authentication setting
    Description: Configure authentication setting.
```

```

set active-auth-scheme {string}
set auth-https [enable|disable]
set captive-portal {string}
set captive-portal-ip {ipv4-address-any}
set captive-portal-ip6 {ipv6-address}
set captive-portal-port {integer}
set captive-portal-ssl-port {integer}
set captive-portal-type [fqdn|ip]
set captive-portal6 {string}
set cert-auth [enable|disable]
set cert-captive-portal {string}
set cert-captive-portal-ip {ipv4-address-any}
set cert-captive-portal-port {integer}
set cookie-max-age {integer}
set cookie-refresh-div {integer}
set dev-range <name1>, <name2>, ...
set ip-auth-cookie [enable|disable]
set persistent-cookie [enable|disable]
set sso-auth-scheme {string}
set update-time {user}
set user-cert-ca <name1>, <name2>, ...
end

```

config authentication setting

Parameter	Description	Type	Size	Default
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35	
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
captive-portal	Captive portal host name.	string	Maximum length: 255	
captive-portal-ip	Captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0
captive-portal-ip6	Captive portal IPv6 address.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
captive-portal-port	Captive portal port number (1 - 65535, default = 7830).	integer	Minimum value: 1 Maximum value: 65535	7830
captive-portal-ssl-port	Captive portal SSL port number (1 - 65535, default = 7831).	integer	Minimum value: 1 Maximum value: 65535	7831
captive-portal-type	Captive portal type.	option	-	fqdn
	Option	Description		
	fqdn	Use FQDN for captive portal.		
	ip	Use an IP address for captive portal.		
captive-portal6	IPv6 captive portal host name.	string	Maximum length: 255	
cert-auth	Enable/disable redirecting certificate authentication to HTTPS portal.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
cert-captive-portal	Certificate captive portal host name.	string	Maximum length: 255	
cert-captive-portal-ip	Certificate captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0
cert-captive-portal-port	Certificate captive portal port number (1 - 65535, default = 7832).	integer	Minimum value: 1 Maximum value: 65535	7832
cookie-max-age	Persistent web portal cookie maximum age in minutes (30 - 10080 (1 week), default = 480 (8 hours)).	integer	Minimum value: 30 Maximum value: 10080	480

Parameter	Description	Type	Size	Default						
cookie-refresh-div	Refresh rate divider of persistent web portal cookie (default = 2). Refresh value = cookie-max-age/cookie-refresh-div.	integer	Minimum value: 2 Maximum value: 4	2						
dev-range <name>	Address range for the IP based device query. Address name.	string	Maximum length: 79							
ip-auth-cookie	Enable/disable persistent cookie on IP based web portal authentication (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable persistent cookie for IP-based authentication.</td></tr><tr><td>disable</td><td>Disable persistent cookie for IP-based authentication.</td></tr></table>	Option	Description	enable	Enable persistent cookie for IP-based authentication.	disable	Disable persistent cookie for IP-based authentication.			
Option	Description									
enable	Enable persistent cookie for IP-based authentication.									
disable	Disable persistent cookie for IP-based authentication.									
persistent-cookie	Enable/disable persistent cookie on web portal authentication (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable persistent cookie.</td></tr><tr><td>disable</td><td>Disable persistent cookie.</td></tr></table>	Option	Description	enable	Enable persistent cookie.	disable	Disable persistent cookie.			
Option	Description									
enable	Enable persistent cookie.									
disable	Disable persistent cookie.									
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35							
update-time	Time of the last update.	user	Not Specified							
user-cert-ca <name>	CA certificate used for client certificate verification. CA certificate list.	string	Maximum length: 79							

automation

This section includes syntax for the following commands:

- [config automation setting on page 184](#)

config automation setting

Automation setting configuration.

```
config automation setting
  Description: Automation setting configuration.
  set fabric-sync [enable|disable]
  set max-concurrent-stitches {integer}
end
```

config automation setting

Parameter	Description	Type	Size	Default						
fabric-sync	Enable/disable synchronization of automation settings with security fabric.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Synchronize automation setting with security fabric.</td></tr><tr><td>disable</td><td>Do not synchronize automation setting with security fabric.</td></tr></table>				Option	Description	enable	Synchronize automation setting with security fabric.	disable	Do not synchronize automation setting with security fabric.
	Option	Description								
	enable	Synchronize automation setting with security fabric.								
disable	Do not synchronize automation setting with security fabric.									
max-concurrent-stitches	Maximum number of automation stitches that are allowed to run concurrently.	integer	Minimum value: 32 Maximum value: 1024 **	512 **						

** Values may differ between models.

aws

This section includes syntax for the following commands:

- [config aws vpce on page 185](#)

config aws vpce



This command is available for model(s): FortiGate-VM64 AWS.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure AWS VPC configuration.

```
config aws vpce
  Description: Configure AWS VPC configuration.
  edit <id>
    set endpoint-id {string}
    set name {string}
    set vdom {string}
  next
end
```

config aws vpce

Parameter	Description	Type	Size	Default
endpoint-id	VPC endpoint ID.	string	Maximum length: 32	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	VPC endpoint name.	string	Maximum length: 63	
vdom	VDOM name.	string	Maximum length: 31	

azure

This section includes syntax for the following commands:

- [config azure migration on page 187](#)
- [config azure nva on page 188](#)
- [config azure vwan-ingress-public-IPs on page 189](#)
- [config azure vwan-slb on page 190](#)

config azure migration



This command is available for model(s): FortiGate-VM64 Azure.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Azure post live migration process.

```
config azure migration
    Description: Azure post live migration process.
    set auto-reboot [enable|disable]
end
```

config azure migration

Parameter	Description	Type	Size	Default
auto-reboot	Enable/disable automatic reboot after a live migration finishes	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatic reboot after live migration		
	<i>disable</i>	Disable automatic reboot after live migration		

config azure nva



This command is available for model(s): FortiGate-VM64 Azure.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Azure vWAN NVA info from cloudinit.

```
config azure nva
  Description: Azure vWAN NVA info from cloudinit.
end
```

config azure vwan-ingress-public-IPs



This command is available for model(s): FortiGate-VM64 Azure.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Display Azure vWAN SLB ingress public IPs.

```
config azure vwan-ingress-public-IPs
  Description: Display Azure vWAN SLB ingress public IPs.
  edit <name>
    set ip {string}
  next
end
```

config azure vwan-ingress-public-IPs

Parameter	Description	Type	Size	Default
ip	Public IP address.	string	Maximum length: 15	
name	Name of public IP.	string	Maximum length: 127	

config azure vwan-slb



This command is available for model(s): FortiGate-VM64 Azure.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure Azure vWAN slb setting.

```
config azure vwan-slb
  Description: Configure Azure vWAN slb setting.
  set mode [passive|active]
  config permanent-security-rules
    Description: Configure permanent security rules.
    config rules
      Description: Configure security rules.
      edit <name>
        set applies-on {string}
        set destination-port-ranges {string}
        set protocol [TCP|UDP]
        set source-address-prefix {string}
      next
    end
    set status [disable|enable|...]
    set version {integer}
  end
  config temporary-security-rules
    Description: Configure temporary security rules.
    set expiration-time {string}
    config rules
      Description: Configure security rules.
```

```

        edit <name>
            set destination-port-ranges {string}
            set protocol [TCP|UDP]
            set source-address-prefix {string}
        next
    end
    set status [disable|enable|...]
end
end

```

config azure vwan-slb

Parameter	Description	Type	Size	Default
mode	Mode of VWAN SLB setting.	option	-	passive
	Option	Description		
	passive	VWAN SLB setting is passive.		
	active	VWAN SLB setting is active for pushing to online.		

config permanent-security-rules

Parameter	Description	Type	Size	Default
status	Status of SLB inbound security rules setting (read-only).	option	-	disable
	Option	Description		
	<i>disable</i>	SLB inbound security rule is disabled.		
	<i>enable</i>	SLB inbound security rule is enabled.		
	<i>updating</i>	SLB inbound security rule is updating.		
	<i>pending</i>	SLB inbound security rule is pending.		
version	Version of SLB setting (read-only).	integer	Minimum value: 0 0 Maximum value: 4294967295	0

config rules

Parameter	Description	Type	Size	Default
applies-on	Applies on target.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default
destination-port-ranges	Destination port ranges.	string	Maximum length: 127	
name	Name of security rule.	string	Maximum length: 63	
protocol	Protocol.	option	-	TCP
	Option		Description	
	TCP		TCP protocol.	
	UDP		UDP protocol.	
source-address-prefix	Source address ranges.	string	Maximum length: 63	

config temporary-security-rules

Parameter	Description	Type	Size	Default
expiration-time	Expiration time (read-only).	string	Maximum length: 31	
status	Status of SLB inbound security rules setting (read-only).	option	-	disable
	Option		Description	
	disable		SLB inbound security rule is disabled.	
	enable		SLB inbound security rule is enabled.	
	updating		SLB inbound security rule is updating.	
	pending		SLB inbound security rule is pending.	

config rules

Parameter	Description	Type	Size	Default
destination-port-ranges	Destination port ranges.	string	Maximum length: 127	
name	Name of security rule.	string	Maximum length: 63	
protocol	Protocol.	option	-	TCP

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TCP</i>	TCP protocol.		
	<i>UDP</i>	UDP protocol.		
source-address-prefix	Source address ranges.	string	Maximum length: 63	

casb

This section includes syntax for the following commands:

- [config casb attribute-match on page 194](#)
- [config casb profile on page 196](#)
- [config casb saas-application on page 201](#)
- [config casb user-activity on page 204](#)

config casb attribute-match

Configure CASB attribute match rule.

```
config casb attribute-match
  Description: Configure CASB attribute match rule.
  edit <name>
    set application {string}
    config match
      Description: CASB tenant match rules.
      edit <id>
        config rule
          Description: CASB attribute match rule.
          edit <id>
            set attribute {string}
            set case-sensitive [enable|disable]
            set match-pattern [simple|substr|...]
            set match-value {string}
            set negate [enable|disable]
          next
        end
        set rule-strategy [and|or]
      next
    end
    set match-strategy [and|or]
  next
end
```

config casb attribute-match

Parameter	Description	Type	Size	Default
application	CASB attribute application name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
match-strategy	CASB attribute match strategy.	option	-	or
	Option	Description		
	and	Match attribute using a logical AND operator.		
	or	Match attribute using a logical OR operator.		
name	CASB attribute match name.	string	Maximum length: 79	

config match

Parameter	Description	Type	Size	Default						
id	CASB attribute match rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0						
rule-strategy	CASB attribute match rule strategy.	option	-	and						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>and</td><td>Match attribute using a logical AND operator.</td></tr><tr><td>or</td><td>Match attribute using a logical OR operator.</td></tr></table>				Option	Description	and	Match attribute using a logical AND operator.	or	Match attribute using a logical OR operator.
Option	Description									
and	Match attribute using a logical AND operator.									
or	Match attribute using a logical OR operator.									

config rule

Parameter	Description	Type	Size	Default
attribute	CASB attribute match name.	string	Maximum length: 79	
case-sensitive	CASB attribute match case sensitive.	option	-	disable
	Option Description			
	enable	Enable value case sensitive match.		
	disable	Disable value case sensitive match.		
id	CASB attribute rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default								
match-pattern	CASB attribute match pattern.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Exact string match pattern.</td></tr><tr><td><i>substr</i></td><td>Sub-string pattern.</td></tr><tr><td><i>regex</i></td><td>Regular expression pattern.</td></tr></table>	Option	Description	<i>simple</i>	Exact string match pattern.	<i>substr</i>	Sub-string pattern.	<i>regex</i>	Regular expression pattern.			
Option	Description											
<i>simple</i>	Exact string match pattern.											
<i>substr</i>	Sub-string pattern.											
<i>regex</i>	Regular expression pattern.											
match-value	CASB attribute match value.	string	Maximum length: 1023									
negate	Enable/disable what the matching strategy must not be.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Matching strategy is negated.</td></tr><tr><td><i>disable</i></td><td>Matching strategy is not negated.</td></tr></table>	Option	Description	<i>enable</i>	Matching strategy is negated.	<i>disable</i>	Matching strategy is not negated.					
Option	Description											
<i>enable</i>	Matching strategy is negated.											
<i>disable</i>	Matching strategy is not negated.											

config casb profile

Configure CASB profile.

```

config casb profile
  Description: Configure CASB profile.
  edit <name>
    set comment {var-string}
    config saas-application
      Description: CASB profile SaaS application.
      edit <name>
        config access-rule
          Description: CASB profile access rule.
          edit <name>
            set action [monitor|bypass|...]
            config attribute-filter
              Description: CASB profile attribute filter.
              edit <id>
                set action [monitor|bypass|...]
                set attribute-match {string}
              next
            end
            set bypass {option1}, {option2}, ...
          next
        end
      config advanced-tenant-control
        Description: CASB profile advanced tenant control.

```

```

        edit <name>
            config attribute
                Description: CASB advanced tenant control attribute.
                edit <name>
                    set input <value1>, <value2>, ...
                next
            end
        next
    end
    config custom-control
        Description: CASB profile custom control.
        edit <name>
            config attribute-filter
                Description: CASB attribute filter.
                edit <id>
                    set action [monitor|bypass|...]
                    set attribute-match {string}
                next
            end
            config option
                Description: CASB custom control option.
                edit <name>
                    set user-input <value1>, <value2>, ...
                next
            end
        next
    end
    set domain-control [enable|disable]
    set domain-control-domains <name1>, <name2>, ...
    set log [enable|disable]
    set safe-search [enable|disable]
    set safe-search-control <name1>, <name2>, ...
    set status [enable|disable]
    set tenant-control [enable|disable]
    set tenant-control-tenants <name1>, <name2>, ...
next
end
next
end

```

config casb profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	CASB profile name.	string	Maximum length: 47	

config saas-application

Parameter	Description	Type	Size	Default						
domain-control	Enable/disable domain control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
domain-control-domains <name>	CASB profile domain control domains. Domain control domain name.	string	Maximum length: 79							
log	Enable/disable log settings.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable log setting.</td></tr><tr><td>disable</td><td>Disable log setting.</td></tr></table>	Option	Description	enable	Enable log setting.	disable	Disable log setting.			
Option	Description									
enable	Enable log setting.									
disable	Disable log setting.									
name	CASB profile SaaS application name.	string	Maximum length: 79							
safe-search	Enable/disable safe search.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
safe-search-control <name>	CASB profile safe search control. Safe search control name.	string	Maximum length: 79							
status	Enable/disable setting.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
tenant-control	Enable/disable tenant control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr></table>	Option	Description	enable	Enable setting.					
Option	Description									
enable	Enable setting.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable setting.		
tenant-control-tenants <name>	CASB profile tenant control tenants. Tenant control tenants name.	string	Maximum length: 79	

config access-rule

Parameter	Description	Type	Size	Default
action	CASB access rule action.	option	-	monitor
	Option	Description		
	<i>monitor</i>	Log when log is enabled.		
	<i>bypass</i>	Apply bypass options.		
	<i>block</i>	Block the request.		
bypass	CASB bypass options.	option	-	
	Option	Description		
	<i>av</i>	Exempt from AV scanning.		
	<i>dlp</i>	Exempt from data loss prevention (DLP).		
	<i>web-filter</i>	Exempt from web filter.		
	<i>file-filter</i>	Exempt from file filter.		
	<i>video-filter</i>	Exempt from video filter.		
name	CASB access rule activity name.	string	Maximum length: 79	

config attribute-filter

Parameter	Description	Type	Size	Default
action	CASB access rule tenant control action.	option	-	monitor
	Option	Description		
	<i>monitor</i>	Log when log is enabled.		
	<i>bypass</i>	Apply bypass options.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block the request.		
attribute-match	CASB access rule tenant match.	string	Maximum length: 79	
id	CASB tenant control ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config advanced-tenant-control

Parameter	Description	Type	Size	Default
name	CASB advanced tenant control name.	string	Maximum length: 79	

config attribute

Parameter	Description	Type	Size	Default
input <value>	CASB extend user input value. User input value.	string	Maximum length: 79	
name	CASB extend user input name.	string	Maximum length: 79	

config custom-control

Parameter	Description	Type	Size	Default
name	CASB custom control user activity name.	string	Maximum length: 79	

config attribute-filter

Parameter	Description	Type	Size	Default
action	CASB access rule tenant control action.	option	-	monitor
	Option	Description		
	<i>monitor</i>	Log when log is enabled.		
	<i>bypass</i>	Apply bypass options.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block the request.		
attribute-match	CASB access rule tenant match.	string	Maximum length: 79	
id	CASB tenant control ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config option

Parameter	Description	Type	Size	Default
name	CASB custom control option name.	string	Maximum length: 79	
user-input <value>	CASB custom control user input. user input value.	string	Maximum length: 79	

config casb saas-application

Configure CASB SaaS application.

```

config casb saas-application
  Description: Configure CASB SaaS application.
  edit <name>
    set casb-name {string}
    set description {string}
    set domains <domain1>, <domain2>, ...
    config input-attributes
      Description: SaaS application input attributes.
      edit <name>
        set default [string|string-list]
        set description {string}
        set fallback-input [enable|disable]
        set required [enable|disable]
        set type {option}
      next
    end
  config output-attributes
    Description: SaaS application output attributes.
    edit <name>
      set description {string}
      set optional [enable|disable]
      set type [string|string-list|...]
    end
  end
end

```

```

        next
    end
    set status [enable|disable]
    set type [built-in|customized]
    set uuid {string}
next
end

```

config casb saas-application

Parameter	Description	Type	Size	Default						
casb-name	SaaS application signature name.	string	Maximum length: 79							
description	SaaS application description.	string	Maximum length: 63							
domains <domain>	SaaS application domain list. Domain list separated by space.	string	Maximum length: 127							
name	SaaS application name.	string	Maximum length: 79							
status	Enable/disable setting.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
type	SaaS application type.	option	-	customized						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>built-in</i></td><td>Built-in SaaS application.</td></tr><tr><td><i>customized</i></td><td>User customized SaaS application.</td></tr></table>	Option	Description	<i>built-in</i>	Built-in SaaS application.	<i>customized</i>	User customized SaaS application.			
Option	Description									
<i>built-in</i>	Built-in SaaS application.									
<i>customized</i>	User customized SaaS application.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 36							

config input-attributes

Parameter	Description	Type	Size	Default
default	CASB attribute default value.	option	-	string

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>string</i>	String type.		
	<i>string-list</i>	String list type.		
description	CASB attribute description.	string	Maximum length: 63	
fallback-input	CASB attribute legacy input.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
name	CASB attribute name.	string	Maximum length: 79	
required	CASB input attribute required.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
type	CASB attribute format type.	option	-	string
	Option	Description		
	<i>string</i>	String type.		

config output-attributes

Parameter	Description	Type	Size	Default
description	CASB attribute description.	string	Maximum length: 63	
name	CASB attribute name.	string	Maximum length: 79	
optional	CASB output attribute optional.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
type	CASB attribute format type.	option	-	string

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>string</i>	String type.		
	<i>string-list</i>	String list type.		
	<i>integer</i>	Integer type.		
	<i>integer-list</i>	Integer list type.		
	<i>boolean</i>	Boolean type.		

config casb user-activity

Configure CASB user activity.

```

config casb user-activity
  Description: Configure CASB user activity.
  edit <name>
    set application {string}
    set casb-name {string}
    set category [activity-control|tenant-control|...]
    config control-options
      Description: CASB control options.
      edit <name>
        config operations
          Description: CASB control option operations.
          edit <name>
            set action [append|prepend|...]
            set case-sensitive [enable|disable]
            set direction [request|response]
            set header-name {string}
            set search-key {string}
            set search-pattern [simple|substr|...]
            set target [header|path|...]
            set value-from-input [enable|disable]
            set values <value1>, <value2>, ...
          next
        end
        set status [enable|disable]
      next
    end
    set description {string}
    config match
      Description: CASB user activity match rules.
      edit <id>
        config rules
          Description: CASB user activity rules.
          edit <id>

```

```

        set body-type {option}
        set case-sensitive [enable|disable]
        set domains <domain1>, <domain2>, ...
        set header-name {string}
        set jq {string}
        set match-pattern [simple|substr|...]
        set match-value {string}
        set methods <method1>, <method2>, ...
        set negate [enable|disable]
        set type [domains|host|...]
    next
end
set strategy [and|or]
config tenant-extraction
    Description: CASB user activity tenant extraction.
    config filters
        Description: CASB user activity tenant extraction filters.
        edit <id>
            set body-type {option}
            set direction [request|response]
            set header-name {string}
            set place [path|header|...]
        next
    end
    set jq {string}
    set status [disable|enable]
    set type {option}
end
next
end
set match-strategy [and|or]
set status [enable|disable]
set type [built-in|customized]
set uuid {string}
next
end

```

config casb user-activity

Parameter	Description	Type	Size	Default
application	CASB SaaS application name.	string	Maximum length: 79	
casb-name	CASB user activity signature name.	string	Maximum length: 79	
category	CASB user activity category.	option	-	activity-control

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>activity-control</i></td><td>Activity control.</td></tr><tr><td><i>tenant-control</i></td><td>Tenant control.</td></tr><tr><td><i>domain-control</i></td><td>Domain control.</td></tr><tr><td><i>safe-search-control</i></td><td>Safe search control.</td></tr><tr><td><i>other</i></td><td>User customized category.</td></tr></table>	Option	Description	<i>activity-control</i>	Activity control.	<i>tenant-control</i>	Tenant control.	<i>domain-control</i>	Domain control.	<i>safe-search-control</i>	Safe search control.	<i>other</i>	User customized category.			
	Option	Description														
	<i>activity-control</i>	Activity control.														
	<i>tenant-control</i>	Tenant control.														
	<i>domain-control</i>	Domain control.														
	<i>safe-search-control</i>	Safe search control.														
<i>other</i>	User customized category.															
description	CASB user activity description.	string	Maximum length: 63													
match-strategy	CASB user activity match strategy.	option	-	or												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>and</i></td><td>Match user activity using a logical AND operator.</td></tr><tr><td><i>or</i></td><td>Match user activity using a logical OR operator.</td></tr></table>	Option	Description	<i>and</i>	Match user activity using a logical AND operator.	<i>or</i>	Match user activity using a logical OR operator.									
	Option	Description														
	<i>and</i>	Match user activity using a logical AND operator.														
<i>or</i>	Match user activity using a logical OR operator.															
name	CASB user activity name.	string	Maximum length: 79													
status	CASB user activity status.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
type	CASB user activity type.	option	-	customized												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>built-in</i></td><td>Built-in CASB user-activity.</td></tr><tr><td><i>customized</i></td><td>User customized CASB user-activity.</td></tr></table>	Option	Description	<i>built-in</i>	Built-in CASB user-activity.	<i>customized</i>	User customized CASB user-activity.									
	Option	Description														
	<i>built-in</i>	Built-in CASB user-activity.														
<i>customized</i>	User customized CASB user-activity.															
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 36													

config control-options

Parameter	Description	Type	Size	Default						
name	CASB control option name.	string	Maximum length: 79							
status	CASB control option status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config operations

Parameter	Description	Type	Size	Default
action	CASB operation action.	option	-	append
	Option	Description		
	<i>append</i>	Append the values after the target.		
	<i>prepend</i>	Prepend the values before the target.		
	<i>replace</i>	Replace the target by the value.		
	<i>new</i>	Create a new header regardless if existing header is found or not.		
	<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.		
	<i>delete</i>	Delete the target.		
case-sensitive	CASB operation search case sensitive.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable case sensitive search.		
	<i>disable</i>	Disable case sensitive search.		
direction	CASB operation direction.	option	-	request
	Option	Description		
	<i>request</i>	Request.		
	<i>response</i>	Response.		
header-name	CASB operation header name to search.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default								
name	CASB control option operation name.	string	Maximum length: 79									
search-key	CASB operation key to search.	string	Maximum length: 1023									
search-pattern	CASB operation search pattern.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Exact string match pattern.</td></tr><tr><td><i>substr</i></td><td>Sub-string pattern.</td></tr><tr><td><i>regexp</i></td><td>Regular expression pattern.</td></tr></table>	Option	Description	<i>simple</i>	Exact string match pattern.	<i>substr</i>	Sub-string pattern.	<i>regexp</i>	Regular expression pattern.			
Option	Description											
<i>simple</i>	Exact string match pattern.											
<i>substr</i>	Sub-string pattern.											
<i>regexp</i>	Regular expression pattern.											
target	CASB operation target.	option	-	header								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>header</i></td><td>Header.</td></tr><tr><td><i>path</i></td><td>Path.</td></tr><tr><td><i>body</i></td><td>Body.</td></tr></table>	Option	Description	<i>header</i>	Header.	<i>path</i>	Path.	<i>body</i>	Body.			
Option	Description											
<i>header</i>	Header.											
<i>path</i>	Path.											
<i>body</i>	Body.											
value-from-input	Enable/disable value from user input.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable value from input.</td></tr><tr><td><i>disable</i></td><td>Disable value from input.</td></tr></table>	Option	Description	<i>enable</i>	Enable value from input.	<i>disable</i>	Disable value from input.					
Option	Description											
<i>enable</i>	Enable value from input.											
<i>disable</i>	Disable value from input.											
values <value>	CASB operation new values. Operation value.	string	Maximum length: 79									

config match

Parameter	Description	Type	Size	Default
id	CASB user activity match rules ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
strategy	CASB user activity rules strategy.	option	-	and

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>and</i>	Match user activity using a logical AND operator.		
	<i>or</i>	Match user activity using a logical OR operator.		

config rules

Parameter	Description	Type	Size	Default
body-type	CASB user activity match rule body type.	option	-	json
	Option	Description		
	<i>json</i>	JSON body type.		
case-sensitive	CASB user activity match case sensitive.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable value case sensitive match.		
	<i>disable</i>	Disable value case sensitive match.		
domains <domain>	CASB user activity domain list. Domain list separated by space.	string	Maximum length: 127	
header-name	CASB user activity rule header name.	string	Maximum length: 255	
id	CASB user activity rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
jq	CASB user activity rule match jq script.	string	Maximum length: 255	
match-pattern	CASB user activity rule match pattern.	option	-	simple
	Option	Description		
	<i>simple</i>	Exact string match pattern.		
	<i>substr</i>	Sub-string pattern.		
	<i>regex</i>	Regular expression pattern.		
match-value	CASB user activity rule match value.	string	Maximum length: 1023	

Parameter	Description	Type	Size	Default																
methods <method>	CASB user activity method list. User activity method.	string	Maximum length: 79																	
negate	Enable/disable what the matching strategy must not be.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Matching strategy is negated.</td></tr><tr><td><i>disable</i></td><td>Matching strategy is not negated.</td></tr></table>	Option	Description	<i>enable</i>	Matching strategy is negated.	<i>disable</i>	Matching strategy is not negated.													
Option	Description																			
<i>enable</i>	Matching strategy is negated.																			
<i>disable</i>	Matching strategy is not negated.																			
type	CASB user activity rule type.	option	-	host																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>domains</i></td><td>Domains.</td></tr><tr><td><i>host</i></td><td>Host.</td></tr><tr><td><i>path</i></td><td>Path.</td></tr><tr><td><i>header</i></td><td>HTTP header.</td></tr><tr><td><i>header-value</i></td><td>HTTP header and value.</td></tr><tr><td><i>method</i></td><td>HTTP method.</td></tr><tr><td><i>body</i></td><td>HTTP body.</td></tr></table>	Option	Description	<i>domains</i>	Domains.	<i>host</i>	Host.	<i>path</i>	Path.	<i>header</i>	HTTP header.	<i>header-value</i>	HTTP header and value.	<i>method</i>	HTTP method.	<i>body</i>	HTTP body.			
Option	Description																			
<i>domains</i>	Domains.																			
<i>host</i>	Host.																			
<i>path</i>	Path.																			
<i>header</i>	HTTP header.																			
<i>header-value</i>	HTTP header and value.																			
<i>method</i>	HTTP method.																			
<i>body</i>	HTTP body.																			

config tenant-extraction

Parameter	Description	Type	Size	Default						
jq	CASB user activity tenant extraction jq script.	string	Maximum length: 1023							
status	Enable/disable CASB tenant extraction.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable tenant extraction.</td></tr><tr><td><i>enable</i></td><td>Enable tenant extraction.</td></tr></table>	Option	Description	<i>disable</i>	Disable tenant extraction.	<i>enable</i>	Enable tenant extraction.			
Option	Description									
<i>disable</i>	Disable tenant extraction.									
<i>enable</i>	Enable tenant extraction.									
type	CASB user activity tenant extraction type.	option	-	json-query						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>json-query</i></td><td>HTTP JSON body extraction.</td></tr></table>	Option	Description	<i>json-query</i>	HTTP JSON body extraction.					
Option	Description									
<i>json-query</i>	HTTP JSON body extraction.									

config filters

Parameter	Description	Type	Size	Default								
body-type	CASB tenant extraction filter body type.	option	-	json								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>json</i></td><td>JSON body type.</td></tr></table>	Option	Description	<i>json</i>	JSON body type.							
Option	Description											
<i>json</i>	JSON body type.											
direction	CASB tenant extraction filter direction.	option	-	request								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>request</i></td><td>Request.</td></tr><tr><td><i>response</i></td><td>Response.</td></tr></table>	Option	Description	<i>request</i>	Request.	<i>response</i>	Response.					
Option	Description											
<i>request</i>	Request.											
<i>response</i>	Response.											
header-name	CASB tenant extraction filter header name.	string	Maximum length: 255									
id	CASB tenant extraction filter ID.	integer	Minimum value: 0 0 Maximum value: 4294967295									
place	CASB tenant extraction filter place type.	option	-	header								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>path</i></td><td>Path.</td></tr><tr><td><i>header</i></td><td>HTTP header.</td></tr><tr><td><i>body</i></td><td>HTTP body.</td></tr></table>	Option	Description	<i>path</i>	Path.	<i>header</i>	HTTP header.	<i>body</i>	HTTP body.			
Option	Description											
<i>path</i>	Path.											
<i>header</i>	HTTP header.											
<i>body</i>	HTTP body.											

certificate

This section includes syntax for the following commands:

- [config certificate ca on page 212](#)
- [config certificate crl on page 214](#)
- [config certificate hsm-local on page 215](#)
- [config certificate local on page 219](#)
- [config certificate remote on page 224](#)

config certificate ca

CA certificate.

```
config certificate ca
  Description: CA certificate.
  edit <name>
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set ca {user}
    set ca-identifier {string}
    set est-url {string}
    set fabric-ca [disable|enable]
    set obsolete [disable|enable]
    set range [global|vdom]
    set scep-url {string}
    set source [factory|user|...]
    set source-ip {ipv4-address}
    set ssl-inspection-trusted [enable|disable]
  next
end
```

config certificate ca

Parameter	Description	Type	Size	Default
auto-update-days	Number of days to wait before requesting an updated CA certificate (0 - 4294967295, 0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default								
auto-update-days-warning	Number of days before an expiry-warning message is generated (0 - 4294967295, 0 = disabled).	integer	Minimum value: 0 0 Maximum value: 4294967295									
ca	CA certificate as a PEM file.	user	Not Specified									
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255									
est-url	URL of the EST server.	string	Maximum length: 255									
fabric-ca	Enable/disable synchronization of CA across Security Fabric.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable synchronization of CA across Security Fabric.</td></tr><tr><td><i>enable</i></td><td>Enable synchronization of CA across Security Fabric.</td></tr></table>				Option	Description	<i>disable</i>	Disable synchronization of CA across Security Fabric.	<i>enable</i>	Enable synchronization of CA across Security Fabric.		
	Option	Description										
	<i>disable</i>	Disable synchronization of CA across Security Fabric.										
<i>enable</i>	Enable synchronization of CA across Security Fabric.											
name	Name.	string	Maximum length: 79									
obsolete	Enable/disable this CA as obsoleted.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Alive.</td></tr><tr><td><i>enable</i></td><td>Obsolete.</td></tr></table>				Option	Description	<i>disable</i>	Alive.	<i>enable</i>	Obsolete.		
	Option	Description										
	<i>disable</i>	Alive.										
<i>enable</i>	Obsolete.											
range	Either global or VDOM IP address range for the CA certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>				Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.		
	Option	Description										
	<i>global</i>	Global range.										
<i>vdom</i>	VDOM IP address range.											
scep-url	URL of the SCEP server.	string	Maximum length: 255									
source	CA certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>				Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.
	Option	Description										
	<i>factory</i>	Factory installed certificate.										
	<i>user</i>	User generated certificate.										
<i>bundle</i>	Bundle file certificate.											

Parameter	Description	Type	Size	Default
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable
		Option	Description	
		enable	Trusted CA for SSL inspection.	
		disable	Untrusted CA for SSL inspection.	

config certificate crl

Certificate Revocation List as a PEM file.

```

config certificate crl
  Description: Certificate Revocation List as a PEM file.
  edit <name>
    set crl {user}
    set http-url {string}
    set ldap-password {password}
    set ldap-server {string}
    set ldap-username {string}
    set range [global|vdom]
    set scep-cert {string}
    set scep-url {string}
    set source [factory|user|...]
    set source-ip {ipv4-address}
    set update-interval {integer}
    set update-vdom {string}
  next
end

```

config certificate crl

Parameter	Description	Type	Size	Default
crl	Certificate Revocation List as a PEM file.	user	Not Specified	
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255	
ldap-password	LDAP server user password.	password	Not Specified	

Parameter	Description	Type	Size	Default								
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35									
ldap-username	LDAP server user name.	string	Maximum length: 63									
name	Name.	string	Maximum length: 35									
range	Either global or VDOM IP address range for the certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>global</td><td>Global range.</td></tr><tr><td>vdom</td><td>VDOM IP address range.</td></tr></table>				Option	Description	global	Global range.	vdom	VDOM IP address range.		
Option	Description											
global	Global range.											
vdom	VDOM IP address range.											
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL								
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255									
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>factory</td><td>Factory installed certificate.</td></tr><tr><td>user</td><td>User generated certificate.</td></tr><tr><td>bundle</td><td>Bundle file certificate.</td></tr></table>				Option	Description	factory	Factory installed certificate.	user	User generated certificate.	bundle	Bundle file certificate.
Option	Description											
factory	Factory installed certificate.											
user	User generated certificate.											
bundle	Bundle file certificate.											
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0								
update-interval	Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0								
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root								

config certificate hsm-local

Local certificates whose keys are stored on HSM.

```
config certificate hsm-local
  Description: Local certificates whose keys are stored on HSM.
  edit <name>
```

```

set api-version [unknown|gch-default]
set certificate {user}
set comments {string}
set gch-cloud-service-name {string}
set gch-cryptokey {string}
set gch-cryptokey-algorithm [rsa-sign-pkcs1-2048-sha256|rsa-sign-pkcs1-3072-sha256|...]
set gch-cryptokey-version {string}
set gch-keyring {string}
set gch-location {string}
set gch-project {string}
set gch-url {string}
set range [global|vdom]
set source [factory|user|...]
set vendor [unknown|gch]

next
end

```

config certificate hsm-local

Parameter	Description	Type	Size	Default
api-version	API version for communicating with HSM.	option	-	unknown
	Option	Description		
	unknown	Unknown API version.		
	gch-default	Google Cloud HSM default API.		
certificate	PEM format certificate.	user	Not Specified	
comments	Comment.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
gch-cloud-service-name	Cloud service config name to generate access token.	string	Maximum length: 35	
gch-cryptokey	Google Cloud HSM cryptokey.	string	Maximum length: 63	
gch-cryptokey-algorithm	Google Cloud HSM cryptokey algorithm.	option	-	rsa-sign-pkcs1-2048-sha256

Option	Description
<i>rsa-sign-pkcs1-2048-sha256</i>	2048 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.
<i>rsa-sign-pkcs1-3072-sha256</i>	3072 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.
<i>rsa-sign-pkcs1-4096-sha256</i>	4096 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.
<i>rsa-sign-pkcs1-4096-sha512</i>	4096 bit RSA - PKCS#1 v1.5 padding - SHA512 Digest.
<i>rsa-sign-pss-2048-sha256</i>	2048 bit RSA - PSS padding - SHA256 Digest.
<i>rsa-sign-pss-3072-sha256</i>	3072 bit RSA - PSS padding - SHA256 Digest.
<i>rsa-sign-pss-4096-sha256</i>	4096 bit RSA - PSS padding - SHA256 Digest.

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rsa-sign-pss-4096-sha512</i></td><td>4096 bit RSA - PSS padding - SHA256 Digest.</td></tr><tr><td><i>ec-sign-p256-sha256</i></td><td>Elliptic Curve P-256 - SHA256 Digest.</td></tr><tr><td><i>ec-sign-p384-sha384</i></td><td>Elliptic Curve P-384 - SHA384 Digest.</td></tr><tr><td><i>ec-sign-secp256k1-sha256</i></td><td>Elliptic Curvesecp256k1 - SHA256 Digest.</td></tr></table>	Option	Description	<i>rsa-sign-pss-4096-sha512</i>	4096 bit RSA - PSS padding - SHA256 Digest.	<i>ec-sign-p256-sha256</i>	Elliptic Curve P-256 - SHA256 Digest.	<i>ec-sign-p384-sha384</i>	Elliptic Curve P-384 - SHA384 Digest.	<i>ec-sign-secp256k1-sha256</i>	Elliptic Curvesecp256k1 - SHA256 Digest.			
	Option	Description												
	<i>rsa-sign-pss-4096-sha512</i>	4096 bit RSA - PSS padding - SHA256 Digest.												
	<i>ec-sign-p256-sha256</i>	Elliptic Curve P-256 - SHA256 Digest.												
	<i>ec-sign-p384-sha384</i>	Elliptic Curve P-384 - SHA384 Digest.												
<i>ec-sign-secp256k1-sha256</i>	Elliptic Curvesecp256k1 - SHA256 Digest.													
gch-cryptokey-version	Google Cloud HSM cryptokey version.	string	Maximum length: 31											
gch-keyring	Google Cloud HSM keyring.	string	Maximum length: 63											
gch-location	Google Cloud HSM location.	string	Maximum length: 63											
gch-project	Google Cloud HSM project ID.	string	Maximum length: 31											

Parameter	Description	Type	Size	Default								
gch-url	Google Cloud HSM key URL (e.g. "https://cloudkms.googleapis.com/v1/projects/sampleproject/locations/samplelocation/keyRings/samplekeyring/cryptoKeys/sampleKeyName/cryptoKeyVersions/1"). Read-only.	string	Maximum length: 1024									
name	Name.	string	Maximum length: 35									
range	Either a global or VDOM IP address range for the certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>global</td><td>Global range.</td></tr><tr><td>vdom</td><td>VDOM IP address range.</td></tr></table>	Option	Description	global	Global range.	vdom	VDOM IP address range.					
Option	Description											
global	Global range.											
vdom	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>factory</td><td>Factory installed certificate.</td></tr><tr><td>user</td><td>User generated certificate.</td></tr><tr><td>bundle</td><td>Bundle file certificate.</td></tr></table>	Option	Description	factory	Factory installed certificate.	user	User generated certificate.	bundle	Bundle file certificate.			
Option	Description											
factory	Factory installed certificate.											
user	User generated certificate.											
bundle	Bundle file certificate.											
vendor	HSM vendor.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>unknown</td><td>Unknown type of HSM.</td></tr><tr><td>gch</td><td>Google Cloud HSM.</td></tr></table>	Option	Description	unknown	Unknown type of HSM.	gch	Google Cloud HSM.					
Option	Description											
unknown	Unknown type of HSM.											
gch	Google Cloud HSM.											

config certificate local

Local keys and certificates.

```

config certificate local
    Description: Local keys and certificates.
    edit <name>
        set acme-ca-url {string}
        set acme-domain {string}
        set acme-eab-key-hmac {password}
        set acme-eab-key-id {var-string}
        set acme-email {string}
        set acme-renew-window {integer}
        set acme-rsa-key-size {integer}
        set auto-regenerate-days {integer}
        set auto-regenerate-days-warning {integer}
        set ca-identifier {string}
        set certificate {user}
        set cmp-path {string}
        set cmp-regeneration-method [keyupdate|renewal]
        set cmp-server {string}
        set cmp-server-cert {string}
        set comments {string}
        set csr {user}
        set enroll-protocol [none|scep|...]
        set est-ca-id {string}
        set est-client-cert {string}
        set est-http-password {password}
        set est-http-username {string}
        set est-regeneration-method [create-new-key|use-existing-key]
        set est-server {string}
        set est-server-cert {string}
        set est-srp-password {password}
        set est-srp-username {string}
        set ike-localid {string}
        set ike-localid-type [asn1dn|fqdn]
        set name-encoding [printable|utf8]
        set password {password}
        set private-key {user}
        set private-key-retain [enable|disable]
        set range [global|vdom]
        set scep-password {password}
        set scep-url {string}
        set source [factory|user|...]
        set source-ip {ipv4-address}
        set state {user}
    next
end

```

config certificate local

Parameter	Description	Type	Size	Default
acme-ca-url	The URL for the ACME CA server (Let's Encrypt is the default provider).	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory
acme-domain	A valid domain that resolves to this FortiGate unit.	string	Maximum length: 255	
acme-eab-key-hmac	External Account Binding HMAC Key (URL-encoded base64).	password	Not Specified	
acme-eab-key-id	External Account Binding Key ID (optional setting).	var-string	Maximum length: 255	
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255	
acme-renew-window	Beginning of the renewal window (in days before certificate expiration, 30 by default).	integer	Minimum value: 1 Maximum value: 100	30
acme-rsa-key-size	Length of the RSA private key of the generated cert (Minimum 2048 bits).	integer	Minimum value: 2048 Maximum value: 4096	2048
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255	
certificate	PEM format certificate.	user	Not Specified	
cmp-path	Path location inside CMP server.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate
	Option Description			
	keyupate	Key Update.		
	renewal	Renewal.		
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63	
cmp-server-cert	CMP server certificate.	string	Maximum length: 79	
comments	Comment.	string	Maximum length: 511	
csr	Certificate Signing Request.	user	Not Specified	
enroll-protocol	Certificate enrollment protocol.	option	-	none
	Option Description			
	none	None (default).		
	scep	Simple Certificate Enrollment Protocol.		
	cmpv2	Certificate Management Protocol Version 2.		
	acme2	Automated Certificate Management Environment Version 2.		
	est	Enrollment over Secure Transport.		
est-ca-id	CA identifier of the CA server for signing via EST.	string	Maximum length: 255	
est-client-cert	Certificate used to authenticate this FortiGate to EST server.	string	Maximum length: 79	
est-http-password	HTTP Authentication password for signing via EST.	password	Not Specified	
est-http-username	HTTP Authentication username for signing via EST.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
est-regeneration-method	EST behavioral options during re-enrollment.	option	-	create-new-key						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>create-new-key</td><td>Create new private key during re-enrollment.</td></tr><tr><td>use-existing-key</td><td>Reuse existing private key during re-enrollment.</td></tr></table>	Option	Description	create-new-key	Create new private key during re-enrollment.	use-existing-key	Reuse existing private key during re-enrollment.			
Option	Description									
create-new-key	Create new private key during re-enrollment.									
use-existing-key	Reuse existing private key during re-enrollment.									
est-server	Address and port for EST server (e.g. https://example.com:1234).	string	Maximum length: 255							
est-server-cert	EST server's certificate must be verifiable by this certificate to be authenticated.	string	Maximum length: 79							
est-srp-password	EST SRP authentication password.	password	Not Specified							
est-srp-username	EST SRP authentication username.	string	Maximum length: 63							
ike-localid	Local ID the FortiGate uses for authentication as a VPN client.	string	Maximum length: 63							
ike-localid-type	IKE local ID type.	option	-	asn1dn						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>asn1dn</td><td>ASN.1 distinguished name.</td></tr><tr><td>fqdn</td><td>Fully qualified domain name.</td></tr></table>	Option	Description	asn1dn	ASN.1 distinguished name.	fqdn	Fully qualified domain name.			
Option	Description									
asn1dn	ASN.1 distinguished name.									
fqdn	Fully qualified domain name.									
name	Name.	string	Maximum length: 35							
name-encoding	Name encoding method for auto-regeneration.	option	-	printable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>printable</td><td>Printable encoding (default).</td></tr><tr><td>utf8</td><td>UTF-8 encoding.</td></tr></table>	Option	Description	printable	Printable encoding (default).	utf8	UTF-8 encoding.			
Option	Description									
printable	Printable encoding (default).									
utf8	UTF-8 encoding.									

Parameter	Description	Type	Size	Default
password	Password as a PEM file.	password	Not Specified	
private-key	PEM format key encrypted with a password.	user	Not Specified	
private-key-retain	Enable/disable retention of private key during SCEP renewal (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Keep the existing private key during SCEP renewal.		
	<i>disable</i>	Generate a new private key during SCEP renewal.		
range	Either a global or VDOM IP address range for the certificate.	option	-	global
	Option	Description		
	<i>global</i>	Global range.		
	<i>vdom</i>	VDOM IP address range.		
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified	
scep-url	SCEP server URL.	string	Maximum length: 255	
source	Certificate source type.	option	-	user
	Option	Description		
	<i>factory</i>	Factory installed certificate.		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
state	Certificate Signing Request State. Read-only.	user	Not Specified	

config certificate remote

Remote certificate as a PEM file.


```

config certificate remote
    Description: Remote certificate as a PEM file.
    edit <name>
        set range [global|vdom]
        set remote {user}
        set source [factory|user|...]
    next
end

```

config certificate remote

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
range	Either the global or VDOM IP address range for the remote certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
remote	Remote certificate.	user	Not Specified									
source	Remote certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											

diameter-filter

This section includes syntax for the following commands:

- [config diameter-filter profile on page 226](#)

config diameter-filter profile

Configure Diameter filter profiles.

```
config diameter-filter profile
  Description: Configure Diameter filter profiles.
  edit <name>
    set cmd-flags-reserve-set [allow|block|...]
    set command-code-invalid [allow|block|...]
    set command-code-range {user}
    set comment {var-string}
    set log-packet [disable|enable]
    set message-length-invalid [allow|block|...]
    set missing-request-action [allow|block|...]
    set monitor-all-messages [disable|enable]
    set protocol-version-invalid [allow|block|...]
    set request-error-flag-set [allow|block|...]
    set track-requests-answers [disable|enable]
  next
end
```

config diameter-filter profile

Parameter	Description	Type	Size	Default
cmd-flags-reserve-set	Action to be taken for messages with cmd flag reserve bits set.	option	-	block
	Option	Description		
	<i>allow</i>	Allow or pass matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
	<i>monitor</i>	Allow and log matching traffic.		

Parameter	Description	Type	Size	Default
command-code-invalid	Action to be taken for messages with invalid command code.	option	-	block
	Option	Description		
	<i>allow</i>	Allow or pass matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
	<i>monitor</i>	Allow and log matching traffic.		
command-code-range	Valid range for command codes (0-16777215).	user	Not Specified	
comment	Comment.	var-string	Maximum length: 255	
log-packet	Enable/disable packet log for triggered diameter settings.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		
message-length-invalid	Action to be taken for invalid message length.	option	-	block
	Option	Description		
	<i>allow</i>	Allow or pass matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
	<i>monitor</i>	Allow and log matching traffic.		
missing-request-action	Action to be taken for answers without corresponding request.	option	-	block
	Option	Description		
	<i>allow</i>	Allow or pass matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
	<i>monitor</i>	Allow and log matching traffic.		

Parameter	Description	Type	Size	Default										
monitor-all-messages	Enable/disable logging for all User Name and Result Code AVP messages.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>enable</td><td>Enable.</td></tr></table>	Option	Description	disable	Disable.	enable	Enable.							
Option	Description													
disable	Disable.													
enable	Enable.													
name	Profile name.	string	Maximum length: 47											
protocol-version-invalid	Action to be taken for invalid protocol version.	option	-	block										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow or pass matching traffic.</td></tr><tr><td>block</td><td>Block or drop matching traffic.</td></tr><tr><td>reset</td><td>Reset sessions for matching traffic.</td></tr><tr><td>monitor</td><td>Allow and log matching traffic.</td></tr></table>	Option	Description	allow	Allow or pass matching traffic.	block	Block or drop matching traffic.	reset	Reset sessions for matching traffic.	monitor	Allow and log matching traffic.			
Option	Description													
allow	Allow or pass matching traffic.													
block	Block or drop matching traffic.													
reset	Reset sessions for matching traffic.													
monitor	Allow and log matching traffic.													
request-error-flag-set	Action to be taken for request messages with error flag set.	option	-	block										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow or pass matching traffic.</td></tr><tr><td>block</td><td>Block or drop matching traffic.</td></tr><tr><td>reset</td><td>Reset sessions for matching traffic.</td></tr><tr><td>monitor</td><td>Allow and log matching traffic.</td></tr></table>	Option	Description	allow	Allow or pass matching traffic.	block	Block or drop matching traffic.	reset	Reset sessions for matching traffic.	monitor	Allow and log matching traffic.			
Option	Description													
allow	Allow or pass matching traffic.													
block	Block or drop matching traffic.													
reset	Reset sessions for matching traffic.													
monitor	Allow and log matching traffic.													
track-requests-answers	Enable/disable validation that each answer has a corresponding request.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>enable</td><td>Enable.</td></tr></table>	Option	Description	disable	Disable.	enable	Enable.							
Option	Description													
disable	Disable.													
enable	Enable.													

dlp

This section includes syntax for the following commands:

- [config dlp data-type on page 229](#)
- [config dlp dictionary on page 231](#)
- [config dlp exact-data-match on page 233](#)
- [config dlp filepattern on page 234](#)
- [config dlp fp-doc-source on page 238](#)
- [config dlp label on page 241](#)
- [config dlp profile on page 242](#)
- [config dlp sensitivity on page 248](#)
- [config dlp sensor on page 248](#)
- [config dlp settings on page 250](#)

config dlp data-type

Configure predefined data type used by DLP blocking.

```
config dlp data-type
  Description: Configure predefined data type used by DLP blocking.
  edit <name>
    set comment {var-string}
    set look-ahead {integer}
    set look-back {integer}
    set match-ahead {integer}
    set match-around {string}
    set match-back {integer}
    set pattern {string}
    set transform {string}
    set verify {string}
    set verify-transformed-pattern [enable|disable]
    set verify2 {string}
  next
end
```

config dlp data-type

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
look-ahead	Number of characters to obtain in advance for verification (1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255	1						
look-back	Number of characters required to save for verification (1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255	1						
match-ahead	Number of characters behind for match-around (1 - 4096, default = 1).	integer	Minimum value: 1 Maximum value: 4096	1						
match-around	Dictionary to check whether it has a match around (Only support match-any and basic types, no repeat supported).	string	Maximum length: 35							
match-back	Number of characters in front for match-around (1 - 4096, default = 1).	integer	Minimum value: 1 Maximum value: 4096	1						
name	Name of table containing the data type.	string	Maximum length: 35							
pattern	Regular expression pattern string without look around.	string	Maximum length: 255							
transform	Template to transform user input to a pattern using capture group from 'pattern'.	string	Maximum length: 255							
verify	Regular expression pattern string used to verify the data type.	string	Maximum length: 255							
verify-transformed-pattern	Enable/disable verification for transformed pattern.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification for transformed pattern.</td></tr><tr><td><i>disable</i></td><td>Disable verification for transformed pattern.</td></tr></table>				Option	Description	<i>enable</i>	Enable verification for transformed pattern.	<i>disable</i>	Disable verification for transformed pattern.
Option	Description									
<i>enable</i>	Enable verification for transformed pattern.									
<i>disable</i>	Disable verification for transformed pattern.									
verify2	Extra regular expression pattern string used to verify the data type.	string	Maximum length: 255							

config dlp dictionary

Configure dictionaries used by DLP blocking.

```
config dlp dictionary
  Description: Configure dictionaries used by DLP blocking.
  edit <name>
    set comment {var-string}
    config entries
      Description: DLP dictionary entries.
      edit <id>
        set comment {var-string}
        set ignore-case [enable|disable]
        set pattern {string}
        set repeat [enable|disable]
        set status [enable|disable]
        set type {string}
      next
    end
    set match-around [enable|disable]
    set match-type [match-all|match-any]
    set uuid {uuid}
  next
end
```

config dlp dictionary

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
match-around	Enable/disable match-around support.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable match-around support.		
	<i>disable</i>	Disable match-around support.		
match-type	Logical relation between entries (default = match-any).	option	-	match-any
	Option	Description		
	<i>match-all</i>	Match all entries.		
	<i>match-any</i>	Match any entries.		

Parameter	Description	Type	Size	Default
name	Name of table containing the dictionary.	string	Maximum length: 35	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config entries

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
ignore-case	Enable/disable ignore case.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignore case.</td></tr><tr><td><i>disable</i></td><td>Disable ignore case.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignore case.	<i>disable</i>	Disable ignore case.			
Option	Description									
<i>enable</i>	Enable ignore case.									
<i>disable</i>	Disable ignore case.									
pattern	Pattern to match.	string	Maximum length: 255							
repeat	Enable/disable repeat match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable repeat match.</td></tr><tr><td><i>disable</i></td><td>Disable repeat match.</td></tr></table>	Option	Description	<i>enable</i>	Enable repeat match.	<i>disable</i>	Disable repeat match.			
Option	Description									
<i>enable</i>	Enable repeat match.									
<i>disable</i>	Disable repeat match.									
status	Enable/disable this pattern.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this pattern.</td></tr><tr><td><i>disable</i></td><td>Disable this pattern.</td></tr></table>	Option	Description	<i>enable</i>	Enable this pattern.	<i>disable</i>	Disable this pattern.			
Option	Description									
<i>enable</i>	Enable this pattern.									
<i>disable</i>	Disable this pattern.									
type	Pattern type to match.	string	Maximum length: 35							

config dlp exact-data-match

Configure exact-data-match template used by DLP scan.

```
config dlp exact-data-match
  Description: Configure exact-data-match template used by DLP scan.
  edit <name>
    config columns
      Description: DLP exact-data-match column types.
      edit <index>
        set optional [enable|disable]
        set type {string}
      next
    end
    set data {string}
    set optional {integer}
  next
end
```

config dlp exact-data-match

Parameter	Description	Type	Size	Default
data	External resource for exact data match.	string	Maximum length: 35	
name	Name of table containing the exact-data-match template.	string	Maximum length: 35	
optional	Number of optional columns need to match.	integer	Minimum value: 0 Maximum value: 32	0

config columns

Parameter	Description	Type	Size	Default
index	Column index.	integer	Minimum value: 1 Maximum value: 32	0
optional	Enable/disable optional match.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable optional match.	
		<i>disable</i>	Disable optional match.	

Parameter	Description	Type	Size	Default
type	Data-type for this column.	string	Maximum length: 35	

config dlp filepattern

Configure file patterns used by DLP blocking.

```
config dlp filepattern
  Description: Configure file patterns used by DLP blocking.
  edit <id>
    set comment {var-string}
    config entries
      Description: Configure file patterns used by DLP blocking.
      edit <pattern>
        set file-type [7z|arj|...]
        set filter-type [pattern|type]
      next
    end
  set name {string}
next
end
```

config dlp filepattern

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Name of table containing the file pattern list.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default
file-type	Select a file type.	option	-	unknown

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>7z</i>	Match 7-zip files.		
	<i>arj</i>	Match arj compressed files.		
	<i>cab</i>	Match Windows cab files.		
	<i>lzh</i>	Match lzh compressed files.		
	<i>rar</i>	Match rar archives.		
	<i>tar</i>	Match tar files.		
	<i>zip</i>	Match zip files.		
	<i>bzip</i>	Match bzip files.		
	<i>gzip</i>	Match gzip files.		
	<i>bzip2</i>	Match bzip2 files.		
	<i>xz</i>	Match xz files.		
	<i>bat</i>	Match Windows batch files.		
	<i>uue</i>	Match uue files.		
	<i>mime</i>	Match mime files.		
	<i>base64</i>	Match base64 files.		
	<i>binhex</i>	Match binhex files.		
	<i>elf</i>	Match elf files.		
	<i>exe</i>	Match Windows executable files.		
	<i>dll</i>	Match dll files.		
	<i>jnlp</i>	Match jnlp files.		
	<i>hta</i>	Match hta files.		
	<i>html</i>	Match html files.		
	<i>jad</i>	Match jad files.		
	<i>class</i>	Match class files.		
	<i>cod</i>	Match cod files.		
	<i>javascript</i>	Match javascript files.		
	<i>msoffice</i>	Match legacy MS-Office files. doc, ppt, and xls.		
	<i>msoffice</i>	Match MS-Office XML files. docm, docx, pptm, pptx, xlsx, and xlsm.		
	<i>fsg</i>	Match fsg files.		

Parameter	Description	Type	Size	Default

Option	Description
<i>upx</i>	Match upx files.
<i>petite</i>	Match petite files.
<i>aspack</i>	Match aspack files.
<i>sis</i>	Match sis files.
<i>hlp</i>	Match Windows help files.
<i>activemime</i>	Match activemime files.
<i>jpeg</i>	Match jpeg files.
<i>gif</i>	Match gif files.
<i>tiff</i>	Match tiff files.
<i>png</i>	Match png files.
<i>bmp</i>	Match bmp files.
<i>unknown</i>	Match unknown files.
<i>mpeg</i>	Match mpeg files.
<i>mov</i>	Match mov files.
<i>mp3</i>	Match mp3 files.
<i>wma</i>	Match wma files.
<i>wav</i>	Match wav files.
<i>pdf</i>	Match Acrobat PDF files.
<i>avi</i>	Match avi files.
<i>rm</i>	Match rm files.
<i>torrent</i>	Match torrent files.
<i>hibun</i>	Match special-file-23-support files.
<i>msi</i>	Match Windows Installer msi files.
<i>mach-o</i>	Match Mach object files.
<i>dmg</i>	Match Apple disk image files.
<i>.net</i>	Match .NET files.
<i>xar</i>	Match xar archive files.
<i>chm</i>	Match Windows compiled HTML help files.
<i>iso</i>	Match ISO archive files.

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>crx</i></td><td>Match Chrome extension files.</td></tr><tr><td><i>flac</i></td><td>Match flac files.</td></tr><tr><td><i>registry</i></td><td>Match registry files.</td></tr><tr><td><i>hwp</i></td><td>Match hwp files.</td></tr><tr><td><i>rpm</i></td><td>Match rpm files.</td></tr><tr><td><i>c/cpp</i></td><td>Match c/cpp files.</td></tr><tr><td><i>pfile</i></td><td>Match pfile files.</td></tr><tr><td><i>lzip</i></td><td>Match lzip files.</td></tr><tr><td><i>wasm</i></td><td>Match WebAssembly files.</td></tr><tr><td><i>sylk</i></td><td>Match Microsoft symbolic link files.</td></tr><tr><td><i>shellscript</i></td><td>Match shell script files.</td></tr></table>	Option	Description	<i>crx</i>	Match Chrome extension files.	<i>flac</i>	Match flac files.	<i>registry</i>	Match registry files.	<i>hwp</i>	Match hwp files.	<i>rpm</i>	Match rpm files.	<i>c/cpp</i>	Match c/cpp files.	<i>pfile</i>	Match pfile files.	<i>lzip</i>	Match lzip files.	<i>wasm</i>	Match WebAssembly files.	<i>sylk</i>	Match Microsoft symbolic link files.	<i>shellscript</i>	Match shell script files.			
	Option	Description																										
	<i>crx</i>	Match Chrome extension files.																										
	<i>flac</i>	Match flac files.																										
	<i>registry</i>	Match registry files.																										
	<i>hwp</i>	Match hwp files.																										
	<i>rpm</i>	Match rpm files.																										
	<i>c/cpp</i>	Match c/cpp files.																										
	<i>pfile</i>	Match pfile files.																										
	<i>lzip</i>	Match lzip files.																										
	<i>wasm</i>	Match WebAssembly files.																										
<i>sylk</i>	Match Microsoft symbolic link files.																											
<i>shellscript</i>	Match shell script files.																											
filter-type	Filter by file name pattern or by file type.	option	-	pattern																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pattern</i></td><td>Filter by file name pattern.</td></tr><tr><td><i>type</i></td><td>Filter by file type.</td></tr></table>	Option	Description	<i>pattern</i>	Filter by file name pattern.	<i>type</i>	Filter by file type.																					
	Option	Description																										
	<i>pattern</i>	Filter by file name pattern.																										
<i>type</i>	Filter by file type.																											
pattern	Add a file name pattern.	string	Maximum length: 79																									

config dlp fp-doc-source



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Create a DLP fingerprint database by allowing the FortiGate to access a file server containing files from which to create fingerprints.

```
config dlp fp-doc-source
```

Description: Create a DLP fingerprint database by allowing the FortiGate to access a file server containing files from which to create fingerprints.

```
edit <name>
```

```
    set date {integer}
    set file-path {string}
    set file-pattern {string}
    set keep-modified [enable|disable]
    set password {password}
    set period [none|daily|...]
    set remove-deleted [enable|disable]
    set scan-on-creation [enable|disable]
    set scan-subdirectories [enable|disable]
    set sensitivity {string}
    set server {string}
    set server-type {option}
    set tod-hour {integer}
    set tod-min {integer}
    set username {string}
    set vdom [mgmt|current]
    set weekday [sunday|monday|...]
```

```
next
end
```

config dlp fp-doc-source

Parameter	Description	Type	Size	Default
date	Day of the month on which to scan the server (1 - 31).	integer	Minimum value: 1 Maximum value: 31	1
file-path	Path on the server to the fingerprint files (max 119 characters).	string	Maximum length: 119	
file-pattern	Files matching this pattern on the server are fingerprinted. Optionally use the * and ? wildcards.	string	Maximum length: 35	*
keep-modified	Enable so that when a file is changed on the server the FortiGate keeps the old fingerprint and adds a new fingerprint to the database.	option	-	enable
	Option		Description	
	enable		Keep the old fingerprint and add a new fingerprint when a file is changed on the server.	
	disable		Replace the old fingerprint with the new fingerprint when a file is changed on the server.	
name	Name of the DLP fingerprint database.	string	Maximum length: 35	
password	Password required to log into the file server.	password	Not Specified	
period	Frequency for which the FortiGate checks the server for new or changed files.	option	-	none
	Option		Description	
	none		Check the server when the FortiGate starts up.	
	daily		Check the server once a day.	
	weekly		Check the server once a week.	
	monthly		Check the server once a month.	
remove-deleted	Enable to keep the fingerprint database up to date when a file is deleted from the server.	option	-	enable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Keep the fingerprint database up to date when a file is deleted from the server.		
	<i>disable</i>	Do not check for deleted files on the server. Saves system resources.		
scan-on-creation	Enable to keep the fingerprint database up to date when a file is added or changed on the server.	option	-	enable
	Option Description			
	<i>enable</i>	Keep the fingerprint database up to date when a file is added or changed on the server.		
	<i>disable</i>	Do not check for added or changed files on the server. Saves system resources.		
scan-subdirectories	Enable/disable scanning subdirectories to find files to create fingerprints from.	option	-	enable
	Option Description			
	<i>enable</i>	Scan subdirectories.		
	<i>disable</i>	Do not scan subdirectories.		
sensitivity	Select a sensitivity or threat level for matches with this fingerprint database. Add sensitivities using sensitivity.	string	Maximum length: 35	
server	IPv4 or IPv6 address of the server.	string	Maximum length: 35	
server-type	Protocol used to communicate with the file server. Currently only Samba (SMB) servers are supported.	option	-	samba
	Option Description			
	<i>samba</i>	SAMBA server.		
tod-hour	Hour of the day on which to scan the server (0 - 23, default = 1).	integer	Minimum value: 0 Maximum value: 23	1

Parameter	Description	Type	Size	Default																
tod-min	Minute of the hour on which to scan the server (0 - 59).	integer	Minimum value: 0 Maximum value: 59	0																
username	User name required to log into the file server.	string	Maximum length: 35																	
vdom	Select the VDOM that can communicate with the file server.	option	-	mgmt																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mgmt</td><td>Communicate with the file server through the management VDOM.</td></tr><tr><td>current</td><td>Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.</td></tr></table>				Option	Description	mgmt	Communicate with the file server through the management VDOM.	current	Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.										
Option	Description																			
mgmt	Communicate with the file server through the management VDOM.																			
current	Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.																			
weekday	Day of the week on which to scan the server.	option	-	sunday																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sunday</td><td>Sunday</td></tr><tr><td>monday</td><td>Monday</td></tr><tr><td>tuesday</td><td>Tuesday</td></tr><tr><td>wednesday</td><td>Wednesday</td></tr><tr><td>thursday</td><td>Thursday</td></tr><tr><td>friday</td><td>Friday</td></tr><tr><td>saturday</td><td>Saturday</td></tr></table>				Option	Description	sunday	Sunday	monday	Monday	tuesday	Tuesday	wednesday	Wednesday	thursday	Thursday	friday	Friday	saturday	Saturday
Option	Description																			
sunday	Sunday																			
monday	Monday																			
tuesday	Tuesday																			
wednesday	Wednesday																			
thursday	Thursday																			
friday	Friday																			
saturday	Saturday																			

config dlp label

Configure labels used by DLP blocking.

```

config dlp label
  Description: Configure labels used by DLP blocking.
  edit <name>
    set comment {var-string}
    set connector {string}
    config entries
      Description: DLP label entries.
      edit <id>
        set guid {string}
        set mpip-label-name {string}
      next
    end
  end

```

```

        set mpip-type [remote|local]
        set type {option}
    next
end

```

config dlp label

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
connector	Name of SDN connector.	string	Maximum length: 35							
mpip-type	MPIP label type.	option	-	remote						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>remote</i></td><td>Remotely fetched MPIP labels.</td></tr><tr><td><i>local</i></td><td>Locally configured MPIP labels.</td></tr></table>				Option	Description	<i>remote</i>	Remotely fetched MPIP labels.	<i>local</i>	Locally configured MPIP labels.
Option	Description									
<i>remote</i>	Remotely fetched MPIP labels.									
<i>local</i>	Locally configured MPIP labels.									
name	Name of table containing the label.	string	Maximum length: 35							
type	Label type.	option	-	mpip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mpip</i></td><td>Microsoft Purview Information Protection.</td></tr></table>				Option	Description	<i>mpip</i>	Microsoft Purview Information Protection.		
Option	Description									
<i>mpip</i>	Microsoft Purview Information Protection.									

config entries

Parameter	Description	Type	Size	Default
guid	MPIP label guid.	string	Maximum length: 36	
id	ID.	integer	Minimum value: 1 Maximum value: 32	0
mpip-label-name	Name of MPIP label.	string	Maximum length: 127	

config dlp profile

Configure DLP profiles.

```

config dlp profile
  Description: Configure DLP profiles.
  edit <name>
    set comment {var-string}
    set dlp-log [enable|disable]
    set extended-log [enable|disable]
    set feature-set [flow|proxy]
    set full-archive-proto {option1}, {option2}, ...
    set nac-quar-log [enable|disable]
    set replacemsg-group {string}
  config rule
    Description: Set up DLP rules for this profile.
    edit <id>
      set action [allow|log-only|...]
      set archive [disable|enable]
      set expiry {user}
      set file-size {integer}
      set file-type {integer}
      set filter-by [sensor|label|...]
      set label {string}
      set match-percentage {integer}
      set name {string}
      set proto {option1}, {option2}, ...
      set sensitivity <name1>, <name2>, ...
      set sensor <name1>, <name2>, ...
      set severity [info|low|...]
      set type [file|message]
    next
  end
  set summary-proto {option1}, {option2}, ...
next
end

```

config dlp profile

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
dlp-log	Enable/disable DLP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP logging.</td></tr></table>				Option	Description	<i>enable</i>	Enable DLP logging.	<i>disable</i>	Disable DLP logging.
	Option	Description								
	<i>enable</i>	Enable DLP logging.								
<i>disable</i>	Disable DLP logging.									
extended-log	Enable/disable extended logging for data loss prevention.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
feature-set	Flow/proxy feature set.	option	-	flow
	Option Description			
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
full-archive-proto	Protocols to always content archive.	option	-	
	Option Description			
	<i>smtp</i>	SMTP.		
	<i>pop3</i>	POP3.		
	<i>imap</i>	IMAP.		
	<i>http-get</i>	HTTP GET.		
	<i>http-post</i>	HTTP POST.		
	<i>ftp</i>	FTP.		
	<i>nntp</i>	NNTP.		
	<i>mapi</i>	MAPI.		
	<i>ssh</i>	SFTP and SCP.		
	<i>cifs</i>	CIFS.		
nac-quar-log	Enable/disable NAC quarantine logging.	option	-	disable
	Option Description			
	<i>enable</i>	Enable NAC quarantine logging.		
	<i>disable</i>	Disable NAC quarantine logging.		
name	Name of the DLP profile.	string	Maximum length: 47	
replacemsg-group	Replacement message group used by this DLP profile.	string	Maximum length: 35	
summary-proto	Protocols to always log summary.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	smtp	SMTP.		
	pop3	POP3.		
	imap	IMAP.		
	http-get	HTTP GET.		
	http-post	HTTP POST.		
	ftp	FTP.		
	nntp	NNTP.		
	mapi	MAPI.		
	ssh	SFTP and SCP.		
	cifs	CIFS.		

config rule

Parameter	Description	Type	Size	Default										
action	Action to take with content that this DLP profile matches.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the content to pass through the FortiGate and do not create a log message.</td></tr><tr><td>log-only</td><td>Allow the content to pass through the FortiGate, but write a log message.</td></tr><tr><td>block</td><td>Block the content and write a log message.</td></tr><tr><td>quarantine-ip</td><td>Quarantine all traffic from the IP address and write a log message.</td></tr></table>	Option	Description	allow	Allow the content to pass through the FortiGate and do not create a log message.	log-only	Allow the content to pass through the FortiGate, but write a log message.	block	Block the content and write a log message.	quarantine-ip	Quarantine all traffic from the IP address and write a log message.			
Option	Description													
allow	Allow the content to pass through the FortiGate and do not create a log message.													
log-only	Allow the content to pass through the FortiGate, but write a log message.													
block	Block the content and write a log message.													
quarantine-ip	Quarantine all traffic from the IP address and write a log message.													
archive	Enable/disable DLP archiving.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>No DLP archiving.</td></tr><tr><td>enable</td><td>Enable full DLP archiving.</td></tr></table>	Option	Description	disable	No DLP archiving.	enable	Enable full DLP archiving.							
Option	Description													
disable	No DLP archiving.													
enable	Enable full DLP archiving.													
expiry	Quarantine duration in days, hours, minutes (format = dddhhmm).	user	Not Specified	5m										

Parameter	Description	Type	Size	Default
file-size	Match files greater than or equal to this size (KB).	integer	Minimum value: 0 Maximum value: 1644544 **	0
file-type	Select the number of a DLP file pattern table to match.	integer	Minimum value: 0 Maximum value: 4294967295	0
filter-by	Select the type of content to match.	option	-	none
	Option Description			
	sensor	Use DLP sensors to match content.		
	label	Use DLP labels to match content.		
	fingerprint	Match against a fingerprint sensitivity.		
	encrypted	Look for encrypted files.		
	none	No content scan.		
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
label	MIP label.	string	Maximum length: 35	
match-percentage *	Percentage of fingerprints in the fingerprint databases designated with the selected sensitivity to match.	integer	Minimum value: 10 Maximum value: 100	10
name	Filter name.	string	Maximum length: 35	
proto	Check messages or files over one or more of these protocols.	option	-	
	Option Description			
	smtp	SMTP.		
	pop3	POP3.		
	imap	IMAP.		
	http-get	HTTP GET.		
	http-post	HTTP POST.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>ssh</i></td><td>SFTP and SCP.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr></table>	Option	Description	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>mapi</i>	MAPI.	<i>ssh</i>	SFTP and SCP.	<i>cifs</i>	CIFS.			
	Option	Description														
	<i>ftp</i>	FTP.														
	<i>nntp</i>	NNTP.														
	<i>mapi</i>	MAPI.														
	<i>ssh</i>	SFTP and SCP.														
<i>cifs</i>	CIFS.															
sensitivity <name> *	Select a DLP file pattern sensitivity to match. Select a DLP sensitivity.	string	Maximum length: 35													
sensor <name>	Select DLP sensors. Address name.	string	Maximum length: 35													
severity	Select the severity or threat level that matches this filter.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>info</i></td><td>Informational.</td></tr><tr><td><i>low</i></td><td>Low.</td></tr><tr><td><i>medium</i></td><td>Medium.</td></tr><tr><td><i>high</i></td><td>High.</td></tr><tr><td><i>critical</i></td><td>Critical.</td></tr></table>	Option	Description	<i>info</i>	Informational.	<i>low</i>	Low.	<i>medium</i>	Medium.	<i>high</i>	High.	<i>critical</i>	Critical.			
	Option	Description														
	<i>info</i>	Informational.														
	<i>low</i>	Low.														
	<i>medium</i>	Medium.														
	<i>high</i>	High.														
<i>critical</i>	Critical.															
type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).	option	-	file												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>file</i></td><td>Check the contents of downloaded or attached files.</td></tr><tr><td><i>message</i></td><td>Check the contents of email messages, web pages, etc.</td></tr></table>	Option	Description	<i>file</i>	Check the contents of downloaded or attached files.	<i>message</i>	Check the contents of email messages, web pages, etc.									
	Option	Description														
	<i>file</i>	Check the contents of downloaded or attached files.														
<i>message</i>	Check the contents of email messages, web pages, etc.															

* This parameter may not exist in some models.

** Values may differ between models.

config dlp sensitivity



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Create self-explanatory DLP sensitivity levels to be used when setting sensitivity under config fp-doc-source.

```
config dlp sensitivity
    Description: Create self-explanatory DLP sensitivity levels to be used when setting
    sensitivity under config fp-doc-source.
    edit <name>
        next
    end
```

config dlp sensitivity

Parameter	Description	Type	Size	Default
name	DLP Sensitivity Levels.	string	Maximum length: 35	

config dlp sensor

Configure sensors used by DLP blocking.


```

config dlp sensor
  Description: Configure sensors used by DLP blocking.
  edit <name>
    set comment {var-string}
    config entries
      Description: DLP sensor entries.
      edit <id>
        set count {integer}
        set dictionary {string}
        set status [enable|disable]
      next
    end
    set eval {string}
    set match-type [match-all|match-any|...]
  next
end

```

config dlp sensor

Parameter	Description	Type	Size	Default								
comment	Optional comments.	var-string	Maximum length: 255									
eval	Expression to evaluate.	string	Maximum length: 255									
match-type	Logical relation between entries (default = match-any).	option	-	match-any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>match-all</i></td><td>Match all entries.</td></tr><tr><td><i>match-any</i></td><td>Match any entries.</td></tr><tr><td><i>match-eval</i></td><td>Match an expression evaluation.</td></tr></table>				Option	Description	<i>match-all</i>	Match all entries.	<i>match-any</i>	Match any entries.	<i>match-eval</i>	Match an expression evaluation.
	Option	Description										
	<i>match-all</i>	Match all entries.										
	<i>match-any</i>	Match any entries.										
<i>match-eval</i>	Match an expression evaluation.											
name	Name of table containing the sensor.	string	Maximum length: 35									

config entries

Parameter	Description	Type	Size	Default
count	Count of dictionary matches to trigger sensor entry match (Dictionary might not be able to trigger more than once based on its 'repeat' option, 1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255	1

Parameter	Description	Type	Size	Default						
dictionary	Select a DLP dictionary or exact-data-match.	string	Maximum length: 35							
id	ID.	integer	Minimum value: 1 Maximum value: 32	0						
status	Enable/disable this entry.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this entry.</td></tr><tr><td><i>disable</i></td><td>Disable this entry.</td></tr></table>				Option	Description	<i>enable</i>	Enable this entry.	<i>disable</i>	Disable this entry.
Option	Description									
<i>enable</i>	Enable this entry.									
<i>disable</i>	Disable this entry.									

config dlp settings

Configure settings for DLP.

```

config dlp settings
    Description: Configure settings for DLP.
    set cache-mem-percent {integer}
    set chunk-size {integer}
    set config-builder-timeout {integer}
    set db-mode [stop-adding|remove-modified-then-oldest|...]
    set size {integer}
    set storage-device {string}
end

```

config dlp settings

Parameter	Description	Type	Size	Default
cache-mem-percent *	Maximum percentage of available memory allocated to caching DLP fingerprints (1 - 15).	integer	Minimum value: 1 Maximum value: 15	2
chunk-size *	Maximum fingerprint chunk size. Caution, changing this setting will flush the entire database.	integer	Minimum value: 100 Maximum value: 100000	2800
config-builder-timeout	Maximum time allowed for building a single DLP profile (default 60 seconds).	integer	Minimum value: 10 Maximum value: 100000	60

Parameter	Description	Type	Size	Default								
db-mode *	Behavior when the maximum size is reached in the DLP fingerprint database.	option	-	stop-adding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>stop-adding</td><td>Stop adding entries.</td></tr><tr><td>remove-modified-then-oldest</td><td>Remove modified chunks first, then oldest file entries.</td></tr><tr><td>remove-oldest</td><td>Remove the oldest files first.</td></tr></table>				Option	Description	stop-adding	Stop adding entries.	remove-modified-then-oldest	Remove modified chunks first, then oldest file entries.	remove-oldest	Remove the oldest files first.
	Option	Description										
	stop-adding	Stop adding entries.										
	remove-modified-then-oldest	Remove modified chunks first, then oldest file entries.										
remove-oldest	Remove the oldest files first.											
size *	Maximum total size of files within the DLP fingerprint database (MB).	integer	Minimum value: 16 Maximum value: 4294967295	16								
storage-device *	Storage device name.	string	Maximum length: 35									

* This parameter may not exist in some models.

dnsfilter

This section includes syntax for the following commands:

- [config dnsfilter domain-filter on page 252](#)
- [config dnsfilter profile on page 253](#)

config dnsfilter domain-filter

Configure DNS domain filters.

```
config dnsfilter domain-filter
  Description: Configure DNS domain filters.
  edit <id>
    set comment {var-string}
    config entries
      Description: DNS domain filter entries.
      edit <id>
        set action [block|allow|...]
        set domain {string}
        set status [enable|disable]
        set type [simple|regex|...]
      next
    end
  set name {string}
next
end
```

config dnsfilter domain-filter

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default
action	Action to take for domain filter matches.	option	-	block
	Option	Description		
	<i>block</i>	Block DNS requests matching the domain filter.		
	<i>allow</i>	Allow DNS requests matching the domain filter without logging.		
	<i>monitor</i>	Allow DNS requests matching the domain filter with logging.		
domain	Domain entries to be filtered.	string	Maximum length: 511	
id	Id.	integer	Minimum value: 0 0 Maximum value: 4294967295	
status	Enable/disable this domain filter.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this domain filter.		
	<i>disable</i>	Disable this domain filter.		
type	DNS domain filter type.	option	-	simple
	Option	Description		
	<i>simple</i>	Simple domain string.		
	<i>regex</i>	Regular expression domain string.		
	<i>wildcard</i>	Wildcard domain string.		

config dnsfilter profile

Configure DNS domain filter profile.

```
config dnsfilter profile
  Description: Configure DNS domain filter profile.
  edit <name>
    set block-action [block|redirect|...]
    set block-botnet [disable|enable]
    set comment {var-string}
    config dns-translation
      Description: DNS translation settings.
      edit <id>
```

```

        set addr-type [ipv4|ipv6]
        set dst {ipv4-address}
        set dst6 {ipv6-address}
        set netmask {ipv4-netmask}
        set prefix {integer}
        set src {ipv4-address}
        set src6 {ipv6-address}
        set status [enable|disable]
    next
end
config domain-filter
    Description: Domain filter settings.
    set domain-filter-table {integer}
end
set external-ip-blocklist <name1>, <name2>, ...
config ftgd-dns
    Description: FortiGuard DNS Filter settings.
    config filters
        Description: FortiGuard DNS domain filters.
        edit <id>
            set action [block|monitor]
            set category {integer}
            set log [enable|disable]
        next
    end
    set options {option1}, {option2}, ...
end
set log-all-domain [enable|disable]
set redirect-portal {ipv4-address}
set redirect-portal6 {ipv6-address}
set safe-search [disable|enable]
set sdns-domain-log [enable|disable]
set sdns-ftgd-err-log [enable|disable]
set strip-ech [disable|enable]
set transparent-dns-database <name1>, <name2>, ...
set youtube-restrict [strict|moderate|...]
next
end

```

config dnsfilter profile

Parameter	Description	Type	Size	Default
block-action	Action to take for blocked domains.	option	-	redirect
	Option	Description		
	<i>block</i>	Return NXDOMAIN for blocked domains.		
	<i>redirect</i>	Redirect blocked domains to SDNS portal.		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>block-sevrfail</i>	Return SERVFAIL for blocked domains.		
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option	-	disable
	Option Description			
	<i>disable</i>	Disable blocking botnet C&C DNS lookups.		
	<i>enable</i>	Enable blocking botnet C&C DNS lookups.		
comment	Comment.	var-string	Maximum length: 255	
external-ip-blocklist <name>	One or more external IP block lists. External domain block list name.	string	Maximum length: 79	
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-	disable
	Option Description			
	<i>enable</i>	Enable logging of all domains visited.		
	<i>disable</i>	Disable logging of all domains visited.		
name	Profile name.	string	Maximum length: 47	
redirect-portal	IPv4 address of the SDNS redirect portal.	ipv4-address	Not Specified	0.0.0.0
redirect-portal6	IPv6 address of the SDNS redirect portal.	ipv6-address	Not Specified	::
safe-search	Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	option	-	disable
	Option Description			
	<i>disable</i>	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.		
	<i>enable</i>	Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.		
sdns-domain-log	Enable/disable domain filtering and botnet domain logging.	option	-	enable
	Option Description			
	<i>enable</i>	Enable domain filtering and botnet domain logging.		
	<i>disable</i>	Disable domain filtering and botnet domain logging.		

Parameter	Description	Type	Size	Default								
sdns-ftgd-err-log	Enable/disable FortiGuard SDNS rating error logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiGuard SDNS rating error logging.</td></tr><tr><td>disable</td><td>Disable FortiGuard SDNS rating error logging.</td></tr></table>	Option	Description	enable	Enable FortiGuard SDNS rating error logging.	disable	Disable FortiGuard SDNS rating error logging.					
Option	Description											
enable	Enable FortiGuard SDNS rating error logging.											
disable	Disable FortiGuard SDNS rating error logging.											
strip-ech	Enable/disable removal of the encrypted client hello service parameter from supporting DNS RRs.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable removal of the encrypted client hello service parameter from supporting DNS RRs.</td></tr><tr><td>enable</td><td>Enable removal of the encrypted client hello service parameter from supporting DNS RRs.</td></tr></table>	Option	Description	disable	Disable removal of the encrypted client hello service parameter from supporting DNS RRs.	enable	Enable removal of the encrypted client hello service parameter from supporting DNS RRs.					
Option	Description											
disable	Disable removal of the encrypted client hello service parameter from supporting DNS RRs.											
enable	Enable removal of the encrypted client hello service parameter from supporting DNS RRs.											
transparent-dns-database <name>	Transparent DNS database zones. DNS database zone name.	string	Maximum length: 79									
youtube-restrict	Set safe search for YouTube restriction level.	option	-	strict								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>strict</td><td>Enable strict safe search for YouTube.</td></tr><tr><td>moderate</td><td>Enable moderate safe search for YouTube.</td></tr><tr><td>none</td><td>Disable safe search for YouTube.</td></tr></table>	Option	Description	strict	Enable strict safe search for YouTube.	moderate	Enable moderate safe search for YouTube.	none	Disable safe search for YouTube.			
Option	Description											
strict	Enable strict safe search for YouTube.											
moderate	Enable moderate safe search for YouTube.											
none	Disable safe search for YouTube.											

config dns-translation

Parameter	Description	Type	Size	Default						
addr-type	DNS translation type (IPv4 or IPv6).	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 address type.</td></tr><tr><td>ipv6</td><td>IPv6 address type.</td></tr></table>				Option	Description	ipv4	IPv4 address type.	ipv6	IPv6 address type.
Option	Description									
ipv4	IPv4 address type.									
ipv6	IPv6 address type.									

Parameter	Description	Type	Size	Default
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0
dst6	IPv6 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src6.	ipv6-address	Not Specified	::
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified	255.255.255.255
prefix	If src6 and dst6 are subnets rather than single IP addresses, enter the prefix for both src6 and dst6 (1 - 128, default = 128).	integer	Minimum value: 1 1 Maximum value: 128	128
src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified	0.0.0.0
src6	IPv6 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst6.	ipv6-address	Not Specified	::
status	Enable/disable this DNS translation entry.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable this DNS translation.		
	<i>disable</i>	Disable this DNS translation.		

config domain-filter

Parameter	Description	Type	Size	Default
domain-filter-table	DNS domain filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config ftgd-dns

Parameter	Description	Type	Size	Default
options	FortiGuard DNS filter options.	option	-	
	Option	Description		
	<i>error-allow</i>	Allow all domains when FortiGuard DNS servers fail.		
	<i>ftgd-disable</i>	Disable FortiGuard DNS domain rating.		

config filters

Parameter	Description	Type	Size	Default
action	Action to take for DNS requests matching the category.	option	-	monitor
	Option	Description		
	<i>block</i>	Block DNS requests matching the category.		
	<i>monitor</i>	Allow DNS requests matching the category and log the result.		
category	Category number.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default						
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0						
log	Enable/disable DNS filter logging for this DNS profile.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DNS filter logging.</td></tr><tr><td><i>disable</i></td><td>Disable DNS filter logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DNS filter logging.	<i>disable</i>	Disable DNS filter logging.			
Option	Description									
<i>enable</i>	Enable DNS filter logging.									
<i>disable</i>	Disable DNS filter logging.									

dpdk

This section includes syntax for the following commands:

- [config dpdk cpus on page 260](#)
- [config dpdk global on page 262](#)

config dpdk cpus



This command is available for model(s): FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure CPUs enabled to run engines in each DPDK stage.

```
config dpdk cpus
  Description: Configure CPUs enabled to run engines in each DPDK stage.
  set ips-cpus {string}
  set isolated-cpus {string}
  set rx-cpus {string}
  set tx-cpus {string}
  set vnp-cpus {string}
  set vnpsp-cpus {string}
end
```

config dpdk cpus

Parameter	Description	Type	Size	Default
ips-cpus	CPUs enabled to run DPDK IPS engines.	string	Maximum length: 1022	all
isolated-cpus	CPUs isolated to run only the DPDK engines with the exception of processes that have affinity explicitly set by either a user configuration or by their implementation.	string	Maximum length: 1022	none
rx-cpus	CPUs enabled to run DPDK RX engines.	string	Maximum length: 1022	all
tx-cpus	CPUs enabled to run DPDK TX engines.	string	Maximum length: 1022	all
vnp-cpus	CPUs enabled to run DPDK VNP engines.	string	Maximum length: 1022	all
vnpsp-cpus	CPUs enabled to run DPDK VNP slow path.	string	Maximum length: 1022	all

config dpdk global



This command is available for model(s): FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure global DPDK options.

```
config dpdk global
    Description: Configure global DPDK options.
    set elasticbuffer [disable|enable]
    set hugepage-percentage {integer}
    set interface <interface-name1>, <interface-name2>, ...
    set ipsec-offload [disable|enable]
    set multiqueue [disable|enable]
    set per-session-accounting [disable|traffic-log-only|...]
    set protects {string}
    set session-table-percentage {integer}
    set sleep-on-idle [disable|enable]
    set status [disable|enable]
end
```

config dpdk global

Parameter	Description	Type	Size	Default
elasticbuffer	Enable/disable elasticbuffer support for all DPDK ports.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable elasticbuffer support for DPDK ports.		
	<i>enable</i>	Enable elasticbuffer support for DPDK ports.		
hugepage-percentage	Percentage of main memory allocated to hugepages, which are available for DPDK operation.	integer	Minimum value: 15 Maximum value: 50	30
interface <interface-name>	Physical interfaces that enable DPDK. (Only AWS Elastic Network Adapter (ENA) is supported.) Physical interface name. (Only AWS Elastic Network Adapter (ENA) is supported.)	string	Maximum length: 31	
ipsec-offload	Enable/disable DPDK IPsec phase 2 offloading.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable DPDK IPsec phase 2 offloading.		
	<i>enable</i>	Enable DPDK IPsec phase 2 offloading.		
multiqueue	Enable/disable multi-queue RX/TX support for all DPDK ports.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable multi-queue RX/TX support for DPDK ports.		
	<i>enable</i>	Enable multi-queue RX/TX support for DPDK ports.		
per-session-accounting	Enable/disable per-session accounting.	option	-	traffic-log-only
	Option	Description		
	<i>disable</i>	Disable per-session accounting.		
	<i>traffic-log-only</i>	Enable per-session accounting only for VNP sessions with traffic logging turned on in firewall policy.		
	<i>enable</i>	Enable per-session accounting for all VNP sessions. *Affect performance.		
protects	Special arguments for device	string	Maximum length: 2047	

Parameter	Description	Type	Size	Default
session-table-percentage	Percentage of main memory allocated to DPDK session table.	integer	Minimum value: 0 Maximum value: 60	5
sleep-on-idle	Enable/disable sleep-on-idle support for all FDH engines.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable sleep-on-idle support for FDH engines.		
	<i>enable</i>	Enable sleep-on-idle support for FDH engines.		
status	Enable/disable DPDK operation for the entire system.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable DPDK operation.		
	<i>enable</i>	Enable DPDK operation. *The minimum system requirements for DPDK is 2 vCPUs and 4GB memory.		

emailfilter

This section includes syntax for the following commands:

- [config emailfilter block-allow-list on page 265](#)
- [config emailfilter bword on page 267](#)
- [config emailfilter dnsbl on page 269](#)
- [config emailfilter fortishield on page 270](#)
- [config emailfilter iptrust on page 271](#)
- [config emailfilter mheader on page 272](#)
- [config emailfilter options on page 274](#)
- [config emailfilter profile on page 274](#)

config emailfilter block-allow-list

Configure anti-spam block/allow list.

```
config emailfilter block-allow-list
  Description: Configure anti-spam block/allow list.
  edit <id>
    set comment {var-string}
    config entries
      Description: Anti-spam block/allow entries.
      edit <id>
        set action [reject|spam|...]
        set addr-type [ipv4|ipv6]
        set ip4-subnet {ipv4-classnet}
        set ip6-subnet {ipv6-network}
        set pattern {string}
        set pattern-type [wildcard|regexp]
        set status [enable|disable]
        set type [ip|email-to|...]
      next
    end
    set name {string}
  next
end
```

config emailfilter block-allow-list

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default								
action	Reject, mark as spam or good email.	option	-	spam								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reject</i></td><td>Reject the connection.</td></tr><tr><td><i>spam</i></td><td>Mark as spam email.</td></tr><tr><td><i>clear</i></td><td>Mark as good email.</td></tr></table>	Option	Description	<i>reject</i>	Reject the connection.	<i>spam</i>	Mark as spam email.	<i>clear</i>	Mark as good email.			
	Option	Description										
	<i>reject</i>	Reject the connection.										
	<i>spam</i>	Mark as spam email.										
<i>clear</i>	Mark as good email.											
addr-type	IP address type.	option	-	ipv4								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>IPv4 Address type.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 Address type.</td></tr></table>	Option	Description	<i>ipv4</i>	IPv4 Address type.	<i>ipv6</i>	IPv6 Address type.					
	Option	Description										
	<i>ipv4</i>	IPv4 Address type.										
<i>ipv6</i>	IPv6 Address type.											
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
ip4-subnet	IPv4 network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0								
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128								
pattern	Pattern to match.	string	Maximum length: 127									
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regexp</i>	Perl regular expression.		
status	Enable/disable status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
type	Entry type.	option	-	ip
	Option	Description		
	<i>ip</i>	By IP address.		
	<i>email-to</i>	By email recipient.		
	<i>email-from</i>	By email sender.		
	<i>subject</i>	By email subject.		

config emailfilter bword

Configure AntiSpam banned word list.

```

config emailfilter bword
  Description: Configure AntiSpam banned word list.
  edit <id>
    set comment {var-string}
    config entries
      Description: Spam filter banned word.
      edit <id>
        set action [spam|clear]
        set language [western|simch|...]
        set pattern {string}
        set pattern-type [wildcard|regexp]
        set score {integer}
        set status [enable|disable]
        set where [subject|body|...]
      next
    end
    set name {string}
  next
end

```

config emailfilter bword

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default																		
action	Mark spam or good.	option	-	spam																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>spam</td><td>Mark as spam email.</td></tr><tr><td>clear</td><td>Mark as good email.</td></tr></table>	Option	Description	spam	Mark as spam email.	clear	Mark as good email.															
	Option	Description																				
	spam	Mark as spam email.																				
clear	Mark as good email.																					
id	Banned word entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																			
language	Language for the banned word.	option	-	western																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>western</td><td>Western.</td></tr><tr><td>simch</td><td>Simplified Chinese.</td></tr><tr><td>trach</td><td>Traditional Chinese.</td></tr><tr><td>japanese</td><td>Japanese.</td></tr><tr><td>korean</td><td>Korean.</td></tr><tr><td>french</td><td>French.</td></tr><tr><td>thai</td><td>Thai.</td></tr><tr><td>spanish</td><td>Spanish.</td></tr></table>	Option	Description	western	Western.	simch	Simplified Chinese.	trach	Traditional Chinese.	japanese	Japanese.	korean	Korean.	french	French.	thai	Thai.	spanish	Spanish.			
	Option	Description																				
	western	Western.																				
	simch	Simplified Chinese.																				
	trach	Traditional Chinese.																				
	japanese	Japanese.																				
	korean	Korean.																				
	french	French.																				
	thai	Thai.																				
spanish	Spanish.																					
pattern	Pattern for the banned word.	string	Maximum length: 127																			

Parameter	Description	Type	Size	Default
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option	Description		
	wildcard	Wildcard pattern.		
	regex	Perl regular expression.		
score	Score value.	integer	Minimum value: 10 1 Maximum value: 99999	
status	Enable/disable status.	option	-	enable
	Option	Description		
	enable	Enable status.		
	disable	Disable status.		
where	Component of the email to be scanned.	option	-	all
	Option	Description		
	subject	Banned word in email subject.		
	body	Banned word in email body.		
	all	Banned word in both subject and body.		

config emailfilter dnsbl

Configure AntiSpam DNSBL/ORBL.

```

config emailfilter dnsbl
  Description: Configure AntiSpam DNSBL/ORBL.
  edit <id>
    set comment {var-string}
    config entries
      Description: Spam filter DNSBL and ORBL server.
      edit <id>
        set action [reject|spam]
        set server {string}
        set status [enable|disable]
      next
    end
    set name {string}
  next
end

```

config emailfilter dnsbl

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default						
action	Reject connection or mark as spam email.	option	-	spam						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reject</i></td><td>Reject the connection.</td></tr><tr><td><i>spam</i></td><td>Mark as spam email.</td></tr></table>	Option	Description	<i>reject</i>	Reject the connection.	<i>spam</i>	Mark as spam email.			
Option	Description									
<i>reject</i>	Reject the connection.									
<i>spam</i>	Mark as spam email.									
id	DNSBL/ORBL entry ID.	integer	Minimum value: 0 Maximum value: 4294967295							
server	DNSBL or ORBL server name.	string	Maximum length: 127							
status	Enable/disable status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></table>	Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.			
Option	Description									
<i>enable</i>	Enable status.									
<i>disable</i>	Disable status.									

config emailfilter fortishield

Configure FortiGuard - AntiSpam.

```
config emailfilter fortishield
  Description: Configure FortiGuard - AntiSpam.
  set spam-submit-force [enable|disable]
  set spam-submit-srv {string}
```

```

    set spam-submit-txt2htm [enable|disable]
end

```

config emailfilter fortishield

Parameter	Description	Type	Size	Default
spam-submit-force	Enable/disable force insertion of a new mime entity for the submission text.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
spam-submit-srv	Hostname of the spam submission server.	string	Maximum length: 63	www.nospammer.net
spam-submit-txt2htm	Enable/disable conversion of text email to HTML email.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	

config emailfilter iptrust

Configure AntiSpam IP trust.

```

config emailfilter iptrust
    Description: Configure AntiSpam IP trust.
    edit <id>
        set comment {var-string}
        config entries
            Description: Spam filter trusted IP addresses.
            edit <id>
                set addr-type [ipv4|ipv6]
                set ip4-subnet {ipv4-classnet}
                set ip6-subnet {ipv6-network}
                set status [enable|disable]
            next
        end
        set name {string}
    next
end

```

config emailfilter iptrust

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default						
addr-type	Type of address.	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 Address type.</td></tr><tr><td>ipv6</td><td>IPv6 Address type.</td></tr></table>	Option	Description	ipv4	IPv4 Address type.	ipv6	IPv6 Address type.			
	Option	Description								
	ipv4	IPv4 Address type.								
ipv6	IPv6 Address type.									
id	Trusted IP entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
ip4-subnet	IPv4 network address or network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128						
status	Enable/disable status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable status.</td></tr><tr><td>disable</td><td>Disable status.</td></tr></table>	Option	Description	enable	Enable status.	disable	Disable status.			
	Option	Description								
	enable	Enable status.								
disable	Disable status.									

config emailfilter mheader

Configure AntiSpam MIME header.


```

config emailfilter mheader
  Description: Configure AntiSpam MIME header.
  edit <id>
    set comment {var-string}
    config entries
      Description: Spam filter mime header content.
      edit <id>
        set action [spam|clear]
        set fieldbody {string}
        set fieldname {string}
        set pattern-type [wildcard|regexp]
        set status [enable|disable]
      next
    end
    set name {string}
  next
end

```

config emailfilter mheader

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default						
action	Mark spam or good.	option	-	spam						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>spam</i></td><td>Mark as spam email.</td></tr><tr><td><i>clear</i></td><td>Mark as good email.</td></tr></table>				Option	Description	<i>spam</i>	Mark as spam email.	<i>clear</i>	Mark as good email.
	Option	Description								
	<i>spam</i>	Mark as spam email.								
<i>clear</i>	Mark as good email.									
fieldbody	Pattern for the header field body.	string	Maximum length: 127							
fieldname	Pattern for header field name.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default						
id	Mime header entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0						
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wildcard</td><td>Wildcard pattern.</td></tr><tr><td>regex</td><td>Perl regular expression.</td></tr></table>				Option	Description	wildcard	Wildcard pattern.	regex	Perl regular expression.
	Option	Description								
	wildcard	Wildcard pattern.								
regex	Perl regular expression.									
status	Enable/disable status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable status.</td></tr><tr><td>disable</td><td>Disable status.</td></tr></table>				Option	Description	enable	Enable status.	disable	Disable status.
	Option	Description								
	enable	Enable status.								
disable	Disable status.									

config emailfilter options

Configure AntiSpam options.

```
config emailfilter options
    Description: Configure AntiSpam options.
    set dns-timeout {integer}
end
```

config emailfilter options

Parameter	Description	Type	Size	Default
dns-timeout	DNS query time out (1 - 30 sec).	integer	Minimum value: 1 Maximum value: 30	7

config emailfilter profile

Configure Email Filter profiles.

```
config emailfilter profile
    Description: Configure Email Filter profiles.
```

```

edit <name>
    set comment {var-string}
    set external [enable|disable]
    set feature-set [flow|proxy]
    config gmail
        Description: Gmail.
        set log-all [disable|enable]
    end
    config imap
        Description: IMAP.
        set action [pass|tag]
        set log-all [disable|enable]
        set tag-msg {string}
        set tag-type {option1}, {option2}, ...
    end
    config mapi
        Description: MAPI.
        set action [pass|discard]
        set log-all [disable|enable]
    end
    config msn-hotmail
        Description: MSN Hotmail.
        set log-all [disable|enable]
    end
    set options {option1}, {option2}, ...
    config other-webmails
        Description: Other supported webmails.
        set log-all [disable|enable]
    end
    config pop3
        Description: POP3.
        set action [pass|tag]
        set log-all [disable|enable]
        set tag-msg {string}
        set tag-type {option1}, {option2}, ...
    end
    set replacemsg-group {string}
    config smtp
        Description: SMTP.
        set action [pass|tag|...]
        set hdrop [disable|enable]
        set local-override [disable|enable]
        set log-all [disable|enable]
        set tag-msg {string}
        set tag-type {option1}, {option2}, ...
    end
    set spam-bal-table {integer}
    set spam-bword-table {integer}
    set spam-bword-threshold {integer}
    set spam-filtering [enable|disable]
    set spam-iptrust-table {integer}
    set spam-log [disable|enable]

```

```

set spam-log-fortiguard-response [disable|enable]
set spam-mheader-table {integer}
set spam-rbl-table {integer}
config yahoo-mail
    Description: Yahoo! Mail.
    set log-all [disable|enable]
end
next
end

```

config emailfilter profile

Parameter	Description	Type	Size	Default																
comment	Comment.	var-string	Maximum length: 255																	
external	Enable/disable external Email inspection.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.													
Option	Description																			
<i>enable</i>	Enable setting.																			
<i>disable</i>	Disable setting.																			
feature-set	Flow/proxy feature set.	option	-	flow																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>flow</i></td><td>Flow feature set.</td></tr><tr><td><i>proxy</i></td><td>Proxy feature set.</td></tr></table>	Option	Description	<i>flow</i>	Flow feature set.	<i>proxy</i>	Proxy feature set.													
Option	Description																			
<i>flow</i>	Flow feature set.																			
<i>proxy</i>	Proxy feature set.																			
name	Profile name.	string	Maximum length: 47																	
options	Options.	option	-																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bannedword</i></td><td>Content block.</td></tr><tr><td><i>spambal</i></td><td>Block/allow list.</td></tr><tr><td><i>spamfsip</i></td><td>Email IP address FortiGuard AntiSpam block list check.</td></tr><tr><td><i>spamfssubmit</i></td><td>Add FortiGuard AntiSpam spam submission text.</td></tr><tr><td><i>spamfschksum</i></td><td>Email checksum FortiGuard AntiSpam check.</td></tr><tr><td><i>spamfsurl</i></td><td>Email content URL FortiGuard AntiSpam check.</td></tr><tr><td><i>spamhelodns</i></td><td>Email helo/ehlo domain DNS check.</td></tr></table>	Option	Description	<i>bannedword</i>	Content block.	<i>spambal</i>	Block/allow list.	<i>spamfsip</i>	Email IP address FortiGuard AntiSpam block list check.	<i>spamfssubmit</i>	Add FortiGuard AntiSpam spam submission text.	<i>spamfschksum</i>	Email checksum FortiGuard AntiSpam check.	<i>spamfsurl</i>	Email content URL FortiGuard AntiSpam check.	<i>spamhelodns</i>	Email helo/ehlo domain DNS check.			
Option	Description																			
<i>bannedword</i>	Content block.																			
<i>spambal</i>	Block/allow list.																			
<i>spamfsip</i>	Email IP address FortiGuard AntiSpam block list check.																			
<i>spamfssubmit</i>	Add FortiGuard AntiSpam spam submission text.																			
<i>spamfschksum</i>	Email checksum FortiGuard AntiSpam check.																			
<i>spamfsurl</i>	Email content URL FortiGuard AntiSpam check.																			
<i>spamhelodns</i>	Email helo/ehlo domain DNS check.																			

Parameter	Description	Type	Size	Default
	Option Description			
	spamraddrdns	Email return address DNS check.		
	spamrbl	Email DNSBL & ORBL check.		
	spamhdrcheck	Email mime header check.		
	spamfsphish	Email content phishing URL FortiGuard AntiSpam check.		
replacemsg-group	Replacement message group.	string	Maximum length: 35	
spam-bal-table	Anti-spam block/allow list table ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
spam-bword-table	Anti-spam banned word table ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
spam-bword-threshold	Spam banned word threshold.	integer	Minimum value: 10 0 Maximum value: 2147483647	
spam-filtering	Enable/disable spam filtering.	option	-	disable
	Option Description			
	enable	Enable setting.		
	disable	Disable setting.		
spam-iptrust-table	Anti-spam IP trust table ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
spam-log	Enable/disable spam logging for email filtering.	option	-	enable
	Option Description			
	disable	Disable spam logging for email filtering.		
	enable	Enable spam logging for email filtering.		
spam-log-fortiguard-response	Enable/disable logging FortiGuard spam response.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>			Disable logging FortiGuard spam response.
	<i>enable</i>			Enable logging FortiGuard spam response.
spam-mheader-table	Anti-spam MIME header table ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
spam-rbl-table	Anti-spam DNSBL table ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config gmail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option Description			
	<i>disable</i>			Disable logging of all email traffic.
	<i>enable</i>			Enable logging of all email traffic.

config imap

Parameter	Description	Type	Size	Default
action	Action for spam email.	option	-	tag
	Option Description			
	<i>pass</i>			Allow spam email to pass through.
	<i>tag</i>			Tag spam email with configured text in subject or header.
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option Description			
	<i>disable</i>			Disable logging of all email traffic.
	<i>enable</i>			Enable logging of all email traffic.
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam

Parameter	Description	Type	Size	Default
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo
	Option	Description		
	<i>subject</i>	Prepend text to spam email subject.		
	<i>header</i>	Append a user defined mime header to spam email.		
	<i>spaminfo</i>	Append spam info to spam email header.		

config mapi

Parameter	Description	Type	Size	Default
action	Action for spam email.	option	-	pass
	Option	Description		
	<i>pass</i>	Allow spam email to pass through.		
	<i>discard</i>	Discard (block) spam email.		
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

config msn-hotmail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

config other-webmails

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

config pop3

Parameter	Description	Type	Size	Default
action	Action for spam email.	option	-	tag
	Option	Description		
	<i>pass</i>	Allow spam email to pass through.		
	<i>tag</i>	Tag spam email with configured text in subject or header.		
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo
	Option	Description		
	<i>subject</i>	Prepend text to spam email subject.		
	<i>header</i>	Append a user defined mime header to spam email.		
	<i>spaminfo</i>	Append spam info to spam email header.		

config smtp

Parameter	Description	Type	Size	Default
action	Action for spam email.	option	-	discard
	Option	Description		
	<i>pass</i>	Allow spam email to pass through.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tag</td><td>Tag spam email with configured text in subject or header.</td></tr><tr><td>discard</td><td>Discard (block) spam email.</td></tr></table>	Option	Description	tag	Tag spam email with configured text in subject or header.	discard	Discard (block) spam email.					
Option	Description											
tag	Tag spam email with configured text in subject or header.											
discard	Discard (block) spam email.											
hdrip	Enable/disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.</td></tr><tr><td>enable</td><td>Enable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.</td></tr></table>	Option	Description	disable	Disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.	enable	Enable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.					
Option	Description											
disable	Disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.											
enable	Enable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.											
local-override	Enable/disable local filter to override SMTP remote check result.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable local filter to override SMTP remote check result.</td></tr><tr><td>enable</td><td>Enable local filter to override SMTP remote check result.</td></tr></table>	Option	Description	disable	Disable local filter to override SMTP remote check result.	enable	Enable local filter to override SMTP remote check result.					
Option	Description											
disable	Disable local filter to override SMTP remote check result.											
enable	Enable local filter to override SMTP remote check result.											
log-all	Enable/disable logging of all email traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of all email traffic.</td></tr><tr><td>enable</td><td>Enable logging of all email traffic.</td></tr></table>	Option	Description	disable	Disable logging of all email traffic.	enable	Enable logging of all email traffic.					
Option	Description											
disable	Disable logging of all email traffic.											
enable	Enable logging of all email traffic.											
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam								
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>subject</td><td>Prepend text to spam email subject.</td></tr><tr><td>header</td><td>Append a user defined mime header to spam email.</td></tr><tr><td>spaminfo</td><td>Append spam info to spam email header.</td></tr></table>	Option	Description	subject	Prepend text to spam email subject.	header	Append a user defined mime header to spam email.	spaminfo	Append spam info to spam email header.			
Option	Description											
subject	Prepend text to spam email subject.											
header	Append a user defined mime header to spam email.											
spaminfo	Append spam info to spam email header.											

config yahoo-mail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

endpoint-control

This section includes syntax for the following commands:

- [config endpoint-control fctems-override on page 287](#)
- [config endpoint-control fctems on page 283](#)
- [config endpoint-control settings on page 291](#)

config endpoint-control fctems

Configure FortiClient Enterprise Management Server (EMS) entries.

```
config endpoint-control fctems
  Description: Configure FortiClient Enterprise Management Server (EMS) entries.
  edit <ems-id>
    set call-timeout {integer}
    set capabilities {option1}, {option2}, ...
    set cloud-authentication-access-key {password}
    set dirty-reason [none|mismatched-ems-sn]
    set fortinetone-cloud-authentication [enable|disable]
    set https-port {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set name {string}
    set out-of-sync-threshold {integer}
    set pull-malware-hash [enable|disable]
    set pull-sysinfo [enable|disable]
    set pull-tags [enable|disable]
    set pull-vulnerabilities [enable|disable]
    set send-tags-to-all-vdoms [enable|disable]
    set serial-number {string}
    set server {string}
    set source-ip {ipv4-address-any}
    set status [enable|disable]
    set tenant-id {string}
    set trust-ca-cn [enable|disable]
    set verifying-ca {string}
    set websocket-override [enable|disable]
  next
end
```

config endpoint-control fctems

Parameter	Description	Type	Size	Default
call-timeout	FortiClient EMS call timeout in seconds (1 - 180 seconds, default = 30).	integer	Minimum value: 1 Maximum value: 180	30
capabilities	List of EMS capabilities.	option	-	
	Option	Description		
	<i>fabric-auth</i>	Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.		
	<i>silent-approval</i>	Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.		
	<i>websocket</i>	Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.		
	<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.		
	<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.		
	<i>common-tags-api</i>	Can receive tag information from New Common Tags API from EMS.		
	<i>tenant-id</i>	Allow this FortiGate to retrieve Tenant-ID from EMS.		
	<i>client-avatars</i>	Allow this FortiGate to retrieve avatars from EMS by fingerprint.		
	<i>single-vdom-connector</i>	Allow this FortiGate to create a vdom connector to EMS.		
	<i>fgt-sysinfo-api</i>	Allow this FortiGate to send additional info to EMS.		
<i>ztna-server-info</i>	Allow this FortiGate to send vdom's ZTNA server information to EMS.			
cloud-authentication-access-key	FortiClient EMS Cloud multitenancy access key	password	Not Specified	
dirty-reason	Dirty Reason for FortiClient EMS.	option	-	none
	Option	Description		
	<i>none</i>	FortiClient EMS entry not dirty.		
	<i>mismatched-ems-sn</i>	FortiClient EMS entry dirty because EMS SN is mismatched with configured SN.		

Parameter	Description	Type	Size	Default								
ems-id	EMS ID in order (1 - 7).	integer	Minimum value: 1 Maximum value: 7	0								
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable authentication of FortiClient EMS Cloud through FortiCloud account.</td></tr><tr><td>disable</td><td>Disable authentication of FortiClient EMS Cloud through FortiCloud account.</td></tr></table>	Option	Description	enable	Enable authentication of FortiClient EMS Cloud through FortiCloud account.	disable	Disable authentication of FortiClient EMS Cloud through FortiCloud account.					
Option	Description											
enable	Enable authentication of FortiClient EMS Cloud through FortiCloud account.											
disable	Disable authentication of FortiClient EMS Cloud through FortiCloud account.											
https-port	FortiClient EMS HTTPS access port number. (1 - 65535, default: 443).	integer	Minimum value: 1 Maximum value: 65535	443								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
name	FortiClient Enterprise Management Server (EMS) name.	string	Maximum length: 35									
out-of-sync-threshold	Outdated resource threshold in seconds (10 - 3600, default = 180).	integer	Minimum value: 10 Maximum value: 3600	180								
pull-malware-hash	Enable/disable pulling FortiClient malware hash from EMS.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable pulling FortiClient malware hash from EMS.</td></tr><tr><td>disable</td><td>Disable pulling FortiClient malware hash from EMS.</td></tr></table>	Option	Description	enable	Enable pulling FortiClient malware hash from EMS.	disable	Disable pulling FortiClient malware hash from EMS.					
Option	Description											
enable	Enable pulling FortiClient malware hash from EMS.											
disable	Disable pulling FortiClient malware hash from EMS.											

Parameter	Description	Type	Size	Default						
pull-sysinfo	Enable/disable pulling SysInfo from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable pulling FortiClient user SysInfo from EMS.</td></tr><tr><td>disable</td><td>Disable pulling FortiClient user SysInfo from EMS.</td></tr></table>	Option	Description	enable	Enable pulling FortiClient user SysInfo from EMS.	disable	Disable pulling FortiClient user SysInfo from EMS.			
Option	Description									
enable	Enable pulling FortiClient user SysInfo from EMS.									
disable	Disable pulling FortiClient user SysInfo from EMS.									
pull-tags	Enable/disable pulling FortiClient user tags from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable pulling FortiClient user tags from EMS.</td></tr><tr><td>disable</td><td>Disable pulling FortiClient user tags from EMS.</td></tr></table>	Option	Description	enable	Enable pulling FortiClient user tags from EMS.	disable	Disable pulling FortiClient user tags from EMS.			
Option	Description									
enable	Enable pulling FortiClient user tags from EMS.									
disable	Disable pulling FortiClient user tags from EMS.									
pull-vulnerabilities	Enable/disable pulling vulnerabilities from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable pulling client vulnerabilities from EMS.</td></tr><tr><td>disable</td><td>Disable pulling client vulnerabilities from EMS.</td></tr></table>	Option	Description	enable	Enable pulling client vulnerabilities from EMS.	disable	Disable pulling client vulnerabilities from EMS.			
Option	Description									
enable	Enable pulling client vulnerabilities from EMS.									
disable	Disable pulling client vulnerabilities from EMS.									
send-tags-to-all-vdoms	Relax restrictions on tags to send all EMS tags to all VDOMs	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending tags to all vdoms.</td></tr><tr><td>disable</td><td>Disable sending tags to all vdoms.</td></tr></table>	Option	Description	enable	Enable sending tags to all vdoms.	disable	Disable sending tags to all vdoms.			
Option	Description									
enable	Enable sending tags to all vdoms.									
disable	Disable sending tags to all vdoms.									
serial-number	EMS Serial Number.	string	Maximum length: 16							
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255							
source-ip	REST API call source IP.	ipv4-address-any	Not Specified	0.0.0.0						
status	Enable or disable this EMS configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable EMS configuration and operation.</td></tr><tr><td>disable</td><td>Disable EMS configuration and operation.</td></tr></table>	Option	Description	enable	Enable EMS configuration and operation.	disable	Disable EMS configuration and operation.			
Option	Description									
enable	Enable EMS configuration and operation.									
disable	Disable EMS configuration and operation.									

Parameter	Description	Type	Size	Default						
tenant-id	EMS Tenant ID.	string	Maximum length: 32							
trust-ca-cn	Enable/disable trust of the EMS certificate issuer(CA) and common name(CN) for certificate auto-renewal.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Trust EMS certificate CA & CN to automatically renew certificate.</td></tr><tr><td><i>disable</i></td><td>Do not trust EMS certificate CA & CN to automatically renew certificate.</td></tr></table>	Option	Description	<i>enable</i>	Trust EMS certificate CA & CN to automatically renew certificate.	<i>disable</i>	Do not trust EMS certificate CA & CN to automatically renew certificate.			
Option	Description									
<i>enable</i>	Trust EMS certificate CA & CN to automatically renew certificate.									
<i>disable</i>	Do not trust EMS certificate CA & CN to automatically renew certificate.									
verifying-ca	Lowest CA cert on Fortigate in verified EMS cert chain.	string	Maximum length: 79							
websocket-override	Enable/disable override behavior for how this FortiGate unit connects to EMS using a WebSocket connection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).</td></tr><tr><td><i>disable</i></td><td>Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.</td></tr></table>	Option	Description	<i>enable</i>	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).	<i>disable</i>	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.			
Option	Description									
<i>enable</i>	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).									
<i>disable</i>	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.									

config endpoint-control fctems-override

Configure FortiClient Enterprise Management Server (EMS) entries.

```

config endpoint-control fctems-override
  Description: Configure FortiClient Enterprise Management Server (EMS) entries.
  edit <ems-id>
    set call-timeout {integer}
    set capabilities {option1}, {option2}, ...
    set cloud-authentication-access-key {password}
    set dirty-reason [none|mismatched-ems-sn]
    set fortinetone-cloud-authentication [enable|disable]
    set https-port {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set name {string}
    set out-of-sync-threshold {integer}
    set pull-malware-hash [enable|disable]
    set pull-sysinfo [enable|disable]
    set pull-tags [enable|disable]
    set pull-vulnerabilities [enable|disable]
  
```

```

set send-tags-to-all-vdoms [enable|disable]
set serial-number {string}
set server {string}
set source-ip {ipv4-address-any}
set status [enable|disable]
set tenant-id {string}
set trust-ca-cn [enable|disable]
set verifying-ca {string}
set websocket-override [enable|disable]
next
end

```

config endpoint-control fctems-override

Parameter	Description	Type	Size	Default																								
call-timeout	FortiClient EMS call timeout in seconds (1 - 180 seconds, default = 30).	integer	Minimum value: 1 Maximum value: 180	30																								
capabilities	List of EMS capabilities.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fabric-auth</i></td><td>Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.</td></tr><tr><td><i>silent-approval</i></td><td>Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.</td></tr><tr><td><i>websocket</i></td><td>Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.</td></tr><tr><td><i>websocket-malware</i></td><td>Allow this FortiGate unit to request malware hash notifications over websocket.</td></tr><tr><td><i>push-ca-certs</i></td><td>Enable/disable syncing deep inspection certificates with EMS.</td></tr><tr><td><i>common-tags-api</i></td><td>Can receive tag information from New Common Tags API from EMS.</td></tr><tr><td><i>tenant-id</i></td><td>Allow this FortiGate to retrieve Tenant-ID from EMS.</td></tr><tr><td><i>client-avatars</i></td><td>Allow this FortiGate to retrieve avatars from EMS by fingerprint.</td></tr><tr><td><i>single-vdom-connector</i></td><td>Allow this FortiGate to create a vdom connector to EMS.</td></tr><tr><td><i>fgt-sysinfo-api</i></td><td>Allow this FortiGate to send additional info to EMS.</td></tr><tr><td><i>ztna-server-info</i></td><td>Allow this FortiGate to send vdom's ZTNA server information to EMS.</td></tr></table>				Option	Description	<i>fabric-auth</i>	Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.	<i>silent-approval</i>	Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.	<i>websocket</i>	Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.	<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.	<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.	<i>common-tags-api</i>	Can receive tag information from New Common Tags API from EMS.	<i>tenant-id</i>	Allow this FortiGate to retrieve Tenant-ID from EMS.	<i>client-avatars</i>	Allow this FortiGate to retrieve avatars from EMS by fingerprint.	<i>single-vdom-connector</i>	Allow this FortiGate to create a vdom connector to EMS.	<i>fgt-sysinfo-api</i>	Allow this FortiGate to send additional info to EMS.	<i>ztna-server-info</i>	Allow this FortiGate to send vdom's ZTNA server information to EMS.
Option	Description																											
<i>fabric-auth</i>	Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.																											
<i>silent-approval</i>	Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.																											
<i>websocket</i>	Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.																											
<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.																											
<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.																											
<i>common-tags-api</i>	Can receive tag information from New Common Tags API from EMS.																											
<i>tenant-id</i>	Allow this FortiGate to retrieve Tenant-ID from EMS.																											
<i>client-avatars</i>	Allow this FortiGate to retrieve avatars from EMS by fingerprint.																											
<i>single-vdom-connector</i>	Allow this FortiGate to create a vdom connector to EMS.																											
<i>fgt-sysinfo-api</i>	Allow this FortiGate to send additional info to EMS.																											
<i>ztna-server-info</i>	Allow this FortiGate to send vdom's ZTNA server information to EMS.																											

Parameter	Description	Type	Size	Default								
cloud-authentication-access-key	FortiClient EMS Cloud multitenancy access key	password	Not Specified									
dirty-reason	Dirty Reason for FortiClient EMS.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>FortiClient EMS entry not dirty.</td></tr><tr><td>mismatched-ems-sn</td><td>FortiClient EMS entry dirty because EMS SN is mismatched with configured SN.</td></tr></table>				Option	Description	none	FortiClient EMS entry not dirty.	mismatched-ems-sn	FortiClient EMS entry dirty because EMS SN is mismatched with configured SN.		
Option	Description											
none	FortiClient EMS entry not dirty.											
mismatched-ems-sn	FortiClient EMS entry dirty because EMS SN is mismatched with configured SN.											
ems-id	EMS ID in order (1 - 7).	integer	Minimum value: 1 Maximum value: 7	0								
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable authentication of FortiClient EMS Cloud through FortiCloud account.</td></tr><tr><td>disable</td><td>Disable authentication of FortiClient EMS Cloud through FortiCloud account.</td></tr></table>				Option	Description	enable	Enable authentication of FortiClient EMS Cloud through FortiCloud account.	disable	Disable authentication of FortiClient EMS Cloud through FortiCloud account.		
Option	Description											
enable	Enable authentication of FortiClient EMS Cloud through FortiCloud account.											
disable	Disable authentication of FortiClient EMS Cloud through FortiCloud account.											
https-port	FortiClient EMS HTTPS access port number. (1 - 65535, default: 443).	integer	Minimum value: 1 Maximum value: 65535	443								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
name	FortiClient Enterprise Management Server (EMS) name.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
out-of-sync-threshold	Outdated resource threshold in seconds (10 - 3600, default = 180).	integer	Minimum value: 10 Maximum value: 3600	180						
pull-malware-hash	Enable/disable pulling FortiClient malware hash from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient malware hash from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient malware hash from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling FortiClient malware hash from EMS.	<i>disable</i>	Disable pulling FortiClient malware hash from EMS.			
Option	Description									
<i>enable</i>	Enable pulling FortiClient malware hash from EMS.									
<i>disable</i>	Disable pulling FortiClient malware hash from EMS.									
pull-sysinfo	Enable/disable pulling SysInfo from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient user SysInfo from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient user SysInfo from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling FortiClient user SysInfo from EMS.	<i>disable</i>	Disable pulling FortiClient user SysInfo from EMS.			
Option	Description									
<i>enable</i>	Enable pulling FortiClient user SysInfo from EMS.									
<i>disable</i>	Disable pulling FortiClient user SysInfo from EMS.									
pull-tags	Enable/disable pulling FortiClient user tags from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient user tags from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient user tags from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling FortiClient user tags from EMS.	<i>disable</i>	Disable pulling FortiClient user tags from EMS.			
Option	Description									
<i>enable</i>	Enable pulling FortiClient user tags from EMS.									
<i>disable</i>	Disable pulling FortiClient user tags from EMS.									
pull-vulnerabilities	Enable/disable pulling vulnerabilities from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling client vulnerabilities from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling client vulnerabilities from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling client vulnerabilities from EMS.	<i>disable</i>	Disable pulling client vulnerabilities from EMS.			
Option	Description									
<i>enable</i>	Enable pulling client vulnerabilities from EMS.									
<i>disable</i>	Disable pulling client vulnerabilities from EMS.									
send-tags-to-all-vdoms	Relax restrictions on tags to send all EMS tags to all VDOMs	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending tags to all vdoms.</td></tr><tr><td><i>disable</i></td><td>Disable sending tags to all vdoms.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending tags to all vdoms.	<i>disable</i>	Disable sending tags to all vdoms.			
Option	Description									
<i>enable</i>	Enable sending tags to all vdoms.									
<i>disable</i>	Disable sending tags to all vdoms.									
serial-number	EMS Serial Number.	string	Maximum length: 16							

Parameter	Description	Type	Size	Default						
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255							
source-ip	REST API call source IP.	ipv4-address-any	Not Specified	0.0.0.0						
status	Enable or disable this EMS configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable EMS configuration and operation.</td></tr><tr><td>disable</td><td>Disable EMS configuration and operation.</td></tr></table>				Option	Description	enable	Enable EMS configuration and operation.	disable	Disable EMS configuration and operation.
Option	Description									
enable	Enable EMS configuration and operation.									
disable	Disable EMS configuration and operation.									
tenant-id	EMS Tenant ID.	string	Maximum length: 32							
trust-ca-cn	Enable/disable trust of the EMS certificate issuer(CA) and common name(CN) for certificate auto-renewal.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Trust EMS certificate CA & CN to automatically renew certificate.</td></tr><tr><td>disable</td><td>Do not trust EMS certificate CA & CN to automatically renew certificate.</td></tr></table>				Option	Description	enable	Trust EMS certificate CA & CN to automatically renew certificate.	disable	Do not trust EMS certificate CA & CN to automatically renew certificate.
Option	Description									
enable	Trust EMS certificate CA & CN to automatically renew certificate.									
disable	Do not trust EMS certificate CA & CN to automatically renew certificate.									
verifying-ca	Lowest CA cert on Fortigate in verified EMS cert chain.	string	Maximum length: 79							
websocket-override	Enable/disable override behavior for how this FortiGate unit connects to EMS using a WebSocket connection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).</td></tr><tr><td>disable</td><td>Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.</td></tr></table>				Option	Description	enable	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).	disable	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.
Option	Description									
enable	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).									
disable	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.									

config endpoint-control settings

Configure endpoint control settings.

```
config endpoint-control settings
    Description: Configure endpoint control settings.
```

```
set override [enable|disable]
end
```

config endpoint-control settings

Parameter	Description	Type	Size	Default
override	Override global EMS table for this VDOM.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Overriding global EMS table.		
	<i>disable</i>	Disable Overriding global EMS table.		

ethernet-oam

This section includes syntax for the following commands:

- [config ethernet-oam cfm on page 293](#)

config ethernet-oam cfm



This command is available for model(s): FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 200E, FortiGate 200F, FortiGate 201F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F DSL, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

CFM domain configuration.

```
config ethernet-oam cfm
  Description: CFM domain configuration.
  edit <domain-id>
    set domain-level {integer}
    set domain-name {text}
  config service
    Description: CFM service configuration.
    edit <service-id>
      set cos {integer}
      set interface {string}
```

```

        set mepid {integer}
        set message-interval [100|1000|...]
        set sender-id [None|Hostname]
        set service-name {text}
    next
end
next
end

```

config ethernet-oam cfm

Parameter	Description	Type	Size	Default
domain-id	OAM domain ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
domain-level	OAM maintenance level (0 - 7)	integer	Minimum value: 0 0 Maximum value: 7	7
domain-name	OAM domain name. Maintenance Domain Identifier (MDID).	text	Not Specified	

config service

Parameter	Description	Type	Size	Default
cos	Set Class of service (CoS) bit for continuity-check messages. range[0 - 7]	integer	Minimum value: 0 0 Maximum value: 7	0
interface	VLAN interface name where service is enabled	string	Maximum length: 63	
mepid	ID of the local MEP. range[1 - 8191]	integer	Minimum value: 1 1 Maximum value: 8191	1
message-interval	Continuity-check message frequency interval in ms	option	-	1000
	Option		Description	
	100		100 msc	
	1000		1000 msc	
	10000		10000 msc	

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>60000</td><td>60000 msc</td></tr><tr><td>600000</td><td>600000 msc</td></tr></table>	Option	Description	60000	60000 msc	600000	600000 msc			
	Option	Description								
	60000	60000 msc								
	600000	600000 msc								
sender-id	TLV Sender ID. {None Hostname}	option	-	None						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>None</td><td>None</td></tr><tr><td>Hostname</td><td>Hostname</td></tr></table>	Option	Description	None	None	Hostname	Hostname			
	Option	Description								
	None	None								
	Hostname	Hostname								
service-id	Service ID to specify service	integer	Minimum value: 0 0 Maximum value: 4294967295							
service-name	Short MA Name (SMAN)	text	Not Specified							

extension-controller

This section includes syntax for the following commands:

- [config extension-controller dataplan on page 296](#)
- [config extension-controller extender-profile on page 303](#)
- [config extension-controller extender-vap on page 333](#)
- [config extension-controller extender on page 299](#)
- [config extension-controller fortigate-profile on page 338](#)
- [config extension-controller fortigate on page 336](#)

config extension-controller dataplan

FortiExtender dataplan configuration.

```
config extension-controller dataplan
  Description: FortiExtender dataplan configuration.
  edit <name>
    set apn {string}
    set auth-type [none|pap|...]
    set billing-date {integer}
    set capacity {integer}
    set carrier {string}
    set iccid {string}
    set modem-id [modem1|modem2|...]
    set monthly-fee {integer}
    set overage [disable|enable]
    set password {password}
    set pdn [ipv4-only|ipv6-only|...]
    set preferred-subnet {integer}
    set private-network [disable|enable]
    set signal-period {integer}
    set signal-threshold {integer}
    set slot [sim1|sim2]
    set type [carrier|slot|...]
    set username {string}
  next
end
```


config extension-controller dataplan

Parameter	Description	Type	Size	Default								
apn	APN configuration.	string	Maximum length: 63									
auth-type	Authentication type.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No authentication.</td></tr><tr><td><i>pap</i></td><td>PAP.</td></tr><tr><td><i>chap</i></td><td>CHAP.</td></tr></table>	Option	Description	<i>none</i>	No authentication.	<i>pap</i>	PAP.	<i>chap</i>	CHAP.			
Option	Description											
<i>none</i>	No authentication.											
<i>pap</i>	PAP.											
<i>chap</i>	CHAP.											
billing-date	Billing day of the month (1 - 31).	integer	Minimum value: 1 Maximum value: 31	1								
capacity	Capacity in MB (0 - 102400000).	integer	Minimum value: 0 Maximum value: 102400000	0								
carrier	Carrier configuration.	string	Maximum length: 31									
iccid	ICCID configuration.	string	Maximum length: 31									
modem-id	Dataplan's modem specifics, if any.	option	-	all								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>modem1</i></td><td>Modem one.</td></tr><tr><td><i>modem2</i></td><td>Modem two.</td></tr><tr><td><i>all</i></td><td>All modems.</td></tr></table>	Option	Description	<i>modem1</i>	Modem one.	<i>modem2</i>	Modem two.	<i>all</i>	All modems.			
Option	Description											
<i>modem1</i>	Modem one.											
<i>modem2</i>	Modem two.											
<i>all</i>	All modems.											
monthly-fee	Monthly fee of dataplan (0 - 100000, in local currency).	integer	Minimum value: 0 Maximum value: 100000	0								
name	FortiExtender data plan name.	string	Maximum length: 31									
overage	Enable/disable dataplan overage detection.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable dataplan overage detection.		
	<i>enable</i>	Enable dataplan overage detection.		
password	Password.	password	Not Specified	
pdn	PDN type.	option	-	ipv4-only
	Option Description			
	<i>ipv4-only</i>	IPv4 only PDN activation.		
	<i>ipv6-only</i>	IPv6 only PDN activation.		
	<i>ipv4-ipv6</i>	Both IPv4 and IPv6 PDN activations.		
preferred-subnet	Preferred subnet mask (0 - 32).	integer	Minimum value: 0 Maximum value: 32	0
private-network	Enable/disable dataplan private network support.	option	-	disable
	Option Description			
	<i>disable</i>	Disable dataplan private network support.		
	<i>enable</i>	Enable dataplan private network support.		
signal-period	Signal period (600 to 18000 seconds).	integer	Minimum value: 600 Maximum value: 18000	3600
signal-threshold	Signal threshold. Specify the range between 50 - 100, where 50/100 means -50/-100 dBm.	integer	Minimum value: 50 Maximum value: 100	100
slot	SIM slot configuration.	option	-	
	Option Description			
	<i>sim1</i>	Sim slot one.		
	<i>sim2</i>	Sim slot two.		
type	Type preferences configuration.	option	-	generic

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>carrier</i>	Assign by SIM carrier.		
	<i>slot</i>	Assign to SIM slot 1 or 2.		
	<i>iccid</i>	Assign to a specific SIM by ICCID.		
	<i>generic</i>	Compatible with any SIM. Assigned if no other dataplan matches the chosen SIM.		
username	Username.	string	Maximum length: 127	

config extension-controller extender

Extender controller configuration.

```

config extension-controller extender
    Description: Extender controller configuration.
    edit <name>
        set allowaccess {option1}, {option2}, ...
        set authorized [discovered|disable|...]
        set bandwidth-limit {integer}
        set description {string}
        set device-id {integer}
        set enforce-bandwidth [enable|disable]
        set ext-name {string}
        set extension-type [wan-extension|lan-extension]
        set firmware-provision-latest [disable|once]
        set id {string}
        set login-password {password}
        set login-password-change [yes|default|...]
        set override-allowaccess [enable|disable]
        set override-enforce-bandwidth [enable|disable]
        set override-login-password-change [enable|disable]
        set profile {string}
        set vdom {integer}
    config wan-extension
        Description: FortiExtender wan extension configuration.
        set modem1-extension {string}
        set modem1-pdn1-interface {string}
        set modem1-pdn2-interface {string}
        set modem1-pdn3-interface {string}
        set modem1-pdn4-interface {string}
        set modem2-extension {string}
        set modem2-pdn1-interface {string}
        set modem2-pdn2-interface {string}
        set modem2-pdn3-interface {string}

```

```

        set modem2-pdn4-interface {string}
    end
next
end

```

config extension-controller extender

Parameter	Description	Type	Size	Default														
allowaccess	Control management access to the managed extender. Separate entries with a space.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>telnet</i>	TELNET access.	<i>http</i>	HTTP access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.			
Option	Description																	
<i>ping</i>	PING access.																	
<i>telnet</i>	TELNET access.																	
<i>http</i>	HTTP access.																	
<i>https</i>	HTTPS access.																	
<i>ssh</i>	SSH access.																	
<i>snmp</i>	SNMP access.																	
authorized	FortiExtender Administration (enable or disable).	option	-	discovered														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discovered</i></td><td>Controller discovered this FortiExtender.</td></tr><tr><td><i>disable</i></td><td>Controller is configured to not provide service to this FortiExtender.</td></tr><tr><td><i>enable</i></td><td>Controller is configured to provide service to this FortiExtender.</td></tr></table>	Option	Description	<i>discovered</i>	Controller discovered this FortiExtender.	<i>disable</i>	Controller is configured to not provide service to this FortiExtender.	<i>enable</i>	Controller is configured to provide service to this FortiExtender.									
Option	Description																	
<i>discovered</i>	Controller discovered this FortiExtender.																	
<i>disable</i>	Controller is configured to not provide service to this FortiExtender.																	
<i>enable</i>	Controller is configured to provide service to this FortiExtender.																	
bandwidth-limit	FortiExtender LAN extension bandwidth limit (Mbps).	integer	Minimum value: 1024 Maximum value: 16776000															
description	Description.	string	Maximum length: 255															
device-id	Device ID.	integer	Minimum value: 0 Maximum value: 4294967295															
enforce-bandwidth	Enable/disable enforcement of bandwidth on LAN extension interface.	option	-	disable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable to enforce bandwidth limit on LAN extension interface.		
	<i>disable</i>	Disable to enforce bandwidth limit on LAN extension interface.		
ext-name	FortiExtender name.	string	Maximum length: 31	
extension-type	Extension type for this FortiExtender.	option	-	
	Option	Description		
	<i>wan-extension</i>	FortiExtender WAN extension mode.		
	<i>lan-extension</i>	FortiExtender LAN extension mode.		
firmware-provision-latest	Enable/disable one-time automatic provisioning of the latest firmware version.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not automatically provision the latest available firmware.		
	<i>once</i>	Automatically attempt a one-time upgrade to the latest available firmware version.		
id	FortiExtender serial number.	string	Maximum length: 19	
login-password	Set the managed extender's administrator password.	password	Not Specified	
login-password-change	Change or reset the administrator password of a managed extender (yes, default, or no, default = no).	option	-	no
	Option	Description		
	<i>yes</i>	Change the managed extender's administrator password. Use the login-password option to set the password.		
	<i>default</i>	Keep the managed extender's administrator password set to the factory default.		
	<i>no</i>	Do not change the managed extender's administrator password.		
name	FortiExtender entry name.	string	Maximum length: 19	

Parameter	Description	Type	Size	Default						
override-allowaccess	Enable to override the extender profile management access configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the extender profile management access configuration.</td></tr><tr><td>disable</td><td>Use the extender profile management access configuration.</td></tr></table>	Option	Description	enable	Override the extender profile management access configuration.	disable	Use the extender profile management access configuration.			
Option	Description									
enable	Override the extender profile management access configuration.									
disable	Use the extender profile management access configuration.									
override-enforce-bandwidth	Enable to override the extender profile enforce-bandwidth setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable override of FortiExtender profile bandwidth setting.</td></tr><tr><td>disable</td><td>Disable override of FortiExtender profile bandwidth setting.</td></tr></table>	Option	Description	enable	Enable override of FortiExtender profile bandwidth setting.	disable	Disable override of FortiExtender profile bandwidth setting.			
Option	Description									
enable	Enable override of FortiExtender profile bandwidth setting.									
disable	Disable override of FortiExtender profile bandwidth setting.									
override-login-password-change	Enable to override the extender profile login-password (administrator password) setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile login-password (administrator password) setting.</td></tr><tr><td>disable</td><td>Use the the WTP profile login-password (administrator password) setting.</td></tr></table>	Option	Description	enable	Override the WTP profile login-password (administrator password) setting.	disable	Use the the WTP profile login-password (administrator password) setting.			
Option	Description									
enable	Override the WTP profile login-password (administrator password) setting.									
disable	Use the the WTP profile login-password (administrator password) setting.									
profile	FortiExtender profile configuration.	string	Maximum length: 31							
vdom	VDOM. Read-only.	integer	Minimum value: 1 0 Maximum value: 4294967295							

config wan-extension

Parameter	Description	Type	Size	Default
modem1-extension	FortiExtender interface name.	string	Maximum length: 31	
modem1-pdn1-interface	FortiExtender interface name.	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
modem1-pdn2-interface	FortiExtender interface name.	string	Maximum length: 31	
modem1-pdn3-interface	FortiExtender interface name.	string	Maximum length: 31	
modem1-pdn4-interface	FortiExtender interface name.	string	Maximum length: 31	
modem2-extension	FortiExtender interface name.	string	Maximum length: 31	
modem2-pdn1-interface	FortiExtender interface name.	string	Maximum length: 31	
modem2-pdn2-interface	FortiExtender interface name.	string	Maximum length: 31	
modem2-pdn3-interface	FortiExtender interface name.	string	Maximum length: 31	
modem2-pdn4-interface	FortiExtender interface name.	string	Maximum length: 31	

config extension-controller extender-profile

FortiExtender extender profile configuration.

```

config extension-controller extender-profile
  Description: FortiExtender extender profile configuration.
  edit <name>
    set allowaccess {option1}, {option2}, ...
    set bandwidth-limit {integer}
    config cellular
      Description: FortiExtender cellular configuration.
      config controller-report
        Description: FortiExtender controller report configuration.
        set interval {integer}
        set signal-threshold {integer}
        set status [disable|enable]
      end
      set dataplan <name1>, <name2>, ...
    config modem1

```

```

Description: Configuration options for modem 1.
config auto-switch
    Description: FortiExtender auto switch configuration.
    set dataplan [disable|enable]
    set disconnect [disable|enable]
    set disconnect-period {integer}
    set disconnect-threshold {integer}
    set signal [disable|enable]
    set switch-back {option1}, {option2}, ...
    set switch-back-time {string}
    set switch-back-timer {integer}
end
set conn-status {integer}
set default-sim [sim1|sim2|...]
set gps [disable|enable]
set multiple-PDN [disable|enable]
set pdn1-dataplan {string}
set pdn2-dataplan {string}
set pdn3-dataplan {string}
set pdn4-dataplan {string}
set preferred-carrier {string}
set redundant-intf {string}
set redundant-mode [disable|enable]
set sim1-pin [disable|enable]
set sim1-pin-code {password}
set sim2-pin [disable|enable]
set sim2-pin-code {password}
end
config modem2
Description: Configuration options for modem 2.
config auto-switch
    Description: FortiExtender auto switch configuration.
    set dataplan [disable|enable]
    set disconnect [disable|enable]
    set disconnect-period {integer}
    set disconnect-threshold {integer}
    set signal [disable|enable]
    set switch-back {option1}, {option2}, ...
    set switch-back-time {string}
    set switch-back-timer {integer}
end
set conn-status {integer}
set default-sim [sim1|sim2|...]
set gps [disable|enable]
set multiple-PDN [disable|enable]
set pdn1-dataplan {string}
set pdn2-dataplan {string}
set pdn3-dataplan {string}
set pdn4-dataplan {string}
set preferred-carrier {string}
set redundant-intf {string}
set redundant-mode [disable|enable]

```



```

        set sim1-pin [disable|enable]
        set sim1-pin-code {password}
        set sim2-pin [disable|enable]
        set sim2-pin-code {password}
    end
    config sms-notification
        Description: FortiExtender cellular SMS notification configuration.
        config alert
            Description: SMS alert list.
            set data-exhausted {string}
            set fgt-backup-mode-switch {string}
            set low-signal-strength {string}
            set mode-switch {string}
            set os-image-fallback {string}
            set session-disconnect {string}
            set system-reboot {string}
        end
        config receiver
            Description: SMS notification receiver list.
            edit <name>
                set alert {option1}, {option2}, ...
                set phone-number {string}
                set status [disable|enable]
            next
        end
        set status [disable|enable]
    end
end
set enforce-bandwidth [enable|disable]
set extension [wan-extension|lan-extension]
set id {integer}
config lan-extension
    Description: FortiExtender LAN extension configuration.
    config backhaul
        Description: LAN extension backhaul tunnel configuration.
        edit <name>
            set port [wan|lte1|...]
            set role [primary|secondary]
            set weight {integer}
        next
    end
    set backhaul-interface {string}
    set backhaul-ip {string}
    config downlinks
        Description: Config FortiExtender downlink interface for LAN extension.
        edit <name>
            set port [port1|port2|...]
            set pvid {integer}
            set type [port|vap]
            set vap {string}
        next
    end
end

```

```

set ipsec-tunnel {string}
set link-loadbalance [activebackup|loadbalance]
config traffic-split-services
    Description: Config FortiExtender traffic split interface for LAN extension.
    edit <name>
        set address {string}
        set service {string}
        set vsdb [disable|enable]
    next
end
end
set login-password {password}
set login-password-change [yes|default|...]
set model [FX201E|FX211E|...]
config wifi
    Description: FortiExtender Wi-Fi configuration.
    set country [--|AF|...]
    config radio-1
        Description: Radio-1 config for Wi-Fi 2.4GHz
        set 80211d [disable|enable]
        set band {option}
        set bandwidth [auto|20MHz|...]
        set beacon-interval {integer}
        set bss-color {integer}
        set bss-color-mode [auto|static]
        set channel {option1}, {option2}, ...
        set extension-channel [auto|higher|...]
        set guard-interval [auto|400ns|...]
        set lan-ext-vap {string}
        set local-vaps <name1>, <name2>, ...
        set max-clients {integer}
        set mode [AP|Client]
        set operating-standard [auto|11A-N-AC-AX|...]
        set power-level {integer}
        set status [disable|enable]
    end
    config radio-2
        Description: Radio-2 config for Wi-Fi 5GHz
        set 80211d [disable|enable]
        set band {option}
        set bandwidth [auto|20MHz|...]
        set beacon-interval {integer}
        set bss-color {integer}
        set bss-color-mode [auto|static]
        set channel {option1}, {option2}, ...
        set extension-channel [auto|higher|...]
        set guard-interval [auto|400ns|...]
        set lan-ext-vap {string}
        set local-vaps <name1>, <name2>, ...
        set max-clients {integer}
        set mode [AP|Client]
        set operating-standard [auto|11A-N-AC-AX|...]

```

```

        set power-level {integer}
        set status [disable|enable]
    end
end
next
end

```

config extension-controller extender-profile

Parameter	Description	Type	Size	Default														
allowaccess	Control management access to the managed extender. Separate entries with a space.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING access.</td></tr><tr><td>telnet</td><td>TELNET access.</td></tr><tr><td>http</td><td>HTTP access.</td></tr><tr><td>https</td><td>HTTPS access.</td></tr><tr><td>ssh</td><td>SSH access.</td></tr><tr><td>snmp</td><td>SNMP access.</td></tr></table>	Option	Description	ping	PING access.	telnet	TELNET access.	http	HTTP access.	https	HTTPS access.	ssh	SSH access.	snmp	SNMP access.			
Option	Description																	
ping	PING access.																	
telnet	TELNET access.																	
http	HTTP access.																	
https	HTTPS access.																	
ssh	SSH access.																	
snmp	SNMP access.																	
bandwidth-limit	FortiExtender LAN extension bandwidth limit (Mbps).	integer	Minimum value: 1 Maximum value: 16776000	1024														
enforce-bandwidth	Enable/disable enforcement of bandwidth on LAN extension interface.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable to enforce bandwidth limit on LAN extension interface.</td></tr><tr><td>disable</td><td>Disable to enforce bandwidth limit on LAN extension interface.</td></tr></table>	Option	Description	enable	Enable to enforce bandwidth limit on LAN extension interface.	disable	Disable to enforce bandwidth limit on LAN extension interface.											
Option	Description																	
enable	Enable to enforce bandwidth limit on LAN extension interface.																	
disable	Disable to enforce bandwidth limit on LAN extension interface.																	
extension	Extension option.	option	-	wan-extension **														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wan-extension</td><td>WAN extension.</td></tr><tr><td>lan-extension</td><td>LAN extension.</td></tr></table>	Option	Description	wan-extension	WAN extension.	lan-extension	LAN extension.											
Option	Description																	
wan-extension	WAN extension.																	
lan-extension	LAN extension.																	

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 102400000	32
login-password	Set the managed extender's administrator password.	password	Not Specified	
login-password-change	Change or reset the administrator password of a managed extender (yes, default, or no, default = no).	option	-	no
	Option		Description	
	yes	Change the managed extender's administrator password. Use the login-password option to set the password.		
	default	Keep the managed extender's administrator password set to the factory default.		
	no	Do not change the managed extender's administrator password.		
model	Model.	option	-	FX201E
	Option		Description	
	FX201E	FEX-201E model.		
	FX211E	FEX-211E model.		
	FX200F	FEX-200F model.		
	FXA11F	FEX-101F-AM model.		
	FXE11F	FEX-101F-EA model.		
	FXA21F	FEX-201F-AM model.		
	FXE21F	FEX-201F-EA model.		
	FXA22F	FEX-202F-AM model.		
	FXE22F	FEX-202F-EA model.		
	FX212F	FEX-212F model.		
	FX311F	FEX-311F model.		
	FX312F	FEX-312F model.		
	FX511F	FEX-511F model.		
	FXR51G	FER-511G model.		

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>FXN51G</i></td><td>FEX-511G model.</td></tr><tr><td><i>FXW51G</i></td><td>FEX-511G-Wifi model.</td></tr><tr><td><i>FVG21F</i></td><td>FEV-211F model.</td></tr><tr><td><i>FVA21F</i></td><td>FEV-211F-AM model.</td></tr><tr><td><i>FVG22F</i></td><td>FEV-212F model.</td></tr><tr><td><i>FVA22F</i></td><td>FEV-212F-AM model.</td></tr><tr><td><i>FX04DA</i></td><td>FX40D-AMEU model.</td></tr><tr><td><i>FG</i></td><td>FG-CONNECTOR model.</td></tr><tr><td><i>BS10FW</i></td><td>FBS-10FW model.</td></tr><tr><td><i>BS20GW</i></td><td>FBS-20GW model.</td></tr><tr><td><i>BS20GN</i></td><td>FBS-20G model.</td></tr><tr><td><i>FVG51G</i></td><td>FEV-511G model.</td></tr><tr><td><i>FXE11G</i></td><td>FEX-101G model.</td></tr></table>	Option	Description	<i>FXN51G</i>	FEX-511G model.	<i>FXW51G</i>	FEX-511G-Wifi model.	<i>FVG21F</i>	FEV-211F model.	<i>FVA21F</i>	FEV-211F-AM model.	<i>FVG22F</i>	FEV-212F model.	<i>FVA22F</i>	FEV-212F-AM model.	<i>FX04DA</i>	FX40D-AMEU model.	<i>FG</i>	FG-CONNECTOR model.	<i>BS10FW</i>	FBS-10FW model.	<i>BS20GW</i>	FBS-20GW model.	<i>BS20GN</i>	FBS-20G model.	<i>FVG51G</i>	FEV-511G model.	<i>FXE11G</i>	FEX-101G model.			
	Option	Description																														
	<i>FXN51G</i>	FEX-511G model.																														
	<i>FXW51G</i>	FEX-511G-Wifi model.																														
	<i>FVG21F</i>	FEV-211F model.																														
	<i>FVA21F</i>	FEV-211F-AM model.																														
	<i>FVG22F</i>	FEV-212F model.																														
	<i>FVA22F</i>	FEV-212F-AM model.																														
	<i>FX04DA</i>	FX40D-AMEU model.																														
	<i>FG</i>	FG-CONNECTOR model.																														
	<i>BS10FW</i>	FBS-10FW model.																														
	<i>BS20GW</i>	FBS-20GW model.																														
	<i>BS20GN</i>	FBS-20G model.																														
	<i>FVG51G</i>	FEV-511G model.																														
<i>FXE11G</i>	FEX-101G model.																															
name	FortiExtender profile name.	string	Maximum length: 31																													

** Values may differ between models.

config cellular

Parameter	Description	Type	Size	Default
dataplan <name>	Dataplan names. Dataplan name.	string	Maximum length: 79	

config controller-report

Parameter	Description	Type	Size	Default
interval	Controller report interval.	integer	Minimum value: 0 Maximum value: 4294967295	300
signal- threshold	Controller report signal threshold.	integer	Minimum value: 10 Maximum value: 50	10

Parameter	Description	Type	Size	Default
status	FortiExtender controller report status.	option	-	disable
	Option	Description		
	<i>disable</i>	Controller is configured to not provide service to this FortiExtender.		
	<i>enable</i>	Controller is configured to provide service to this FortiExtender.		

config modem1

Parameter	Description	Type	Size	Default
conn-status	Connection status. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
default-sim	Default SIM selection.	option	-	sim1
	Option	Description		
	<i>sim1</i>	Use SIM #1 by default.		
	<i>sim2</i>	Use SIM #2 by default.		
	<i>carrier</i>	Assign default SIM based on carrier.		
	<i>cost</i>	Assign default SIM based on cost.		
gps	FortiExtender GPS enable/disable.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable GPS.		
	<i>enable</i>	Enable GPS.		
multiple-PDN	Multiple-PDN enable/disable.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable multiple PDN.		
	<i>enable</i>	Enable multiple PDN.		
pdn1-dataplan	PDN1-dataplan.	string	Maximum length: 31	
pdn2-dataplan	PDN2-dataplan.	string	Maximum length: 31	
pdn3-dataplan	PDN3-dataplan.	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
pdn4-dataplan	PDN4-dataplan.	string	Maximum length: 31	
preferred-carrier	Preferred carrier.	string	Maximum length: 31	
redundant-intf	Redundant interface.	string	Maximum length: 15	
redundant-mode	FortiExtender mode.	option	-	disable
	Option		Description	
	disable		Disable interface redundancy.	
	enable		Enable interface redundancy.	
sim1-pin	SIM #1 PIN status.	option	-	disable
	Option		Description	
	disable		Disable SIM #1 PIN.	
	enable		Enable SIM #1 PIN.	
sim1-pin-code	SIM #1 PIN password.	password	Not Specified	
sim2-pin	SIM #2 PIN status.	option	-	disable
	Option		Description	
	disable		Disable SIM #2 PIN.	
	enable		Enable SIM #2 PIN.	
sim2-pin-code	SIM #2 PIN password.	password	Not Specified	

config auto-switch

Parameter	Description	Type	Size	Default
dataplan	Automatically switch based on data usage.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable switching of SIM card based on cellular data usage.		
	<i>enable</i>	Enable switching of SIM card based on cellular data usage.		
disconnect	Auto switch by disconnect.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable switching of SIM card based on cellular disconnections.		
	<i>enable</i>	Enable switching of SIM card based on cellular disconnections.		
disconnect-period	Automatically switch based on disconnect period.	integer	Minimum value: 600 Maximum value: 18000	600
disconnect-threshold	Automatically switch based on disconnect threshold.	integer	Minimum value: 1 Maximum value: 100	3
signal	Automatically switch based on signal strength.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable switching of SIM card based on cellular signal quality.		
	<i>enable</i>	Enable switching of SIM card based on cellular signal quality.		
switch-back	Auto switch with switch back multi-options.	option	-	
	Option	Description		
	<i>time</i>	Switch back based on specific time in UTC (HH:MM).		
	<i>timer</i>	Switch back based on an interval.		
switch-back-time	Automatically switch over to preferred SIM/carrier at a specified time in UTC (HH:MM).	string	Maximum length: 31	00:01
switch-back-timer	Automatically switch over to preferred SIM/carrier after the given time (3600 - 2147483647 sec).	integer	Minimum value: 3600 Maximum value: 2147483647	86400

config modem2

Parameter	Description	Type	Size	Default
conn-status	Connection status. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
default-sim	Default SIM selection.	option	-	sim1

Parameter	Description	Type	Size	Default
	Option Description			
	sim1	Use SIM #1 by default.		
	sim2	Use SIM #2 by default.		
	carrier	Assign default SIM based on carrier.		
	cost	Assign default SIM based on cost.		
gps	FortiExtender GPS enable/disable.	option	-	enable
	Option Description			
	disable	Disable GPS.		
	enable	Enable GPS.		
multiple-PDN	Multiple-PDN enable/disable.	option	-	disable
	Option Description			
	disable	Disable multiple PDN.		
	enable	Enable multiple PDN.		
pdn1-dataplan	PDN1-dataplan.	string	Maximum length: 31	
pdn2-dataplan	PDN2-dataplan.	string	Maximum length: 31	
pdn3-dataplan	PDN3-dataplan.	string	Maximum length: 31	
pdn4-dataplan	PDN4-dataplan.	string	Maximum length: 31	
preferred-carrier	Preferred carrier.	string	Maximum length: 31	
redundant-intf	Redundant interface.	string	Maximum length: 15	
redundant-mode	FortiExtender mode.	option	-	disable
	Option Description			
	disable	Disable interface redundancy.		
	enable	Enable interface redundancy.		
sim1-pin	SIM #1 PIN status.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable SIM #1 PIN.		
	<i>enable</i>	Enable SIM #1 PIN.		
sim1-pin-code	SIM #1 PIN password.	password	Not Specified	
sim2-pin	SIM #2 PIN status.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SIM #2 PIN.		
	<i>enable</i>	Enable SIM #2 PIN.		
sim2-pin-code	SIM #2 PIN password.	password	Not Specified	

config auto-switch

Parameter	Description	Type	Size	Default
dataplan	Automatically switch based on data usage.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable switching of SIM card based on cellular data usage.		
	<i>enable</i>	Enable switching of SIM card based on cellular data usage.		
disconnect	Auto switch by disconnect.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable switching of SIM card based on cellular disconnections.		
	<i>enable</i>	Enable switching of SIM card based on cellular disconnections.		
disconnect-period	Automatically switch based on disconnect period.	integer	Minimum value: 600 Maximum value: 18000	600
disconnect-threshold	Automatically switch based on disconnect threshold.	integer	Minimum value: 1 Maximum value: 100	3
signal	Automatically switch based on signal strength.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable switching of SIM card based on cellular signal quality.		
	<i>enable</i>	Enable switching of SIM card based on cellular signal quality.		
switch-back	Auto switch with switch back multi-options.	option	-	
	Option	Description		
	<i>time</i>	Switch back based on specific time in UTC (HH:MM).		
	<i>timer</i>	Switch back based on an interval.		
switch-back-time	Automatically switch over to preferred SIM/carrier at a specified time in UTC (HH:MM).	string	Maximum length: 31	00:01
switch-back-timer	Automatically switch over to preferred SIM/carrier after the given time (3600 - 2147483647 sec).	integer	Minimum value: 3600 Maximum value: 2147483647	86400

config sms-notification

Parameter	Description	Type	Size	Default
status	FortiExtender SMS notification status.	option	-	disable
	Option	Description		
	<i>disable</i>	SMS notification is configured to not provide service to this FortiExtender.		
	<i>enable</i>	SMS notification is configured to provide service to this FortiExtender.		

config alert

Parameter	Description	Type	Size	Default
data-exhausted	Display string when data exhausted.	string	Maximum length: 63	data plan is exhausted
fgt-backup-mode-switch	Display string when FortiGate backup mode switched.	string	Maximum length: 63	FortiGate backup work mode switched
low-signal-strength	Display string when signal strength is low.	string	Maximum length: 63	LTE signal strength is too low

Parameter	Description	Type	Size	Default
mode-switch	Display string when mode is switched.	string	Maximum length: 63	system networking mode switched
os-image-fallback	Display string when falling back to a previous OS image.	string	Maximum length: 63	system start to fallback OS image
session-disconnect	Display string when session disconnected.	string	Maximum length: 63	LTE data session is disconnected
system-reboot	Display string when system rebooted.	string	Maximum length: 63	system will reboot

config receiver

Parameter	Description	Type	Size	Default																
alert	Alert multi-options.	option	-																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>system-reboot</td><td>System will reboot.</td></tr><tr><td>data-exhausted</td><td>Data plan is exhausted.</td></tr><tr><td>session-disconnect</td><td>LTE data session is disconnected.</td></tr><tr><td>low-signal-strength</td><td>LTE signal strength is too low.</td></tr><tr><td>mode-switch</td><td>System is starting to use fallback OS image.</td></tr><tr><td>os-image-fallback</td><td>System networking mode switched.</td></tr><tr><td>fgt-backup-mode-switch</td><td>FortiGate backup work mode switched.</td></tr></table>	Option	Description	system-reboot	System will reboot.	data-exhausted	Data plan is exhausted.	session-disconnect	LTE data session is disconnected.	low-signal-strength	LTE signal strength is too low.	mode-switch	System is starting to use fallback OS image.	os-image-fallback	System networking mode switched.	fgt-backup-mode-switch	FortiGate backup work mode switched.			
Option	Description																			
system-reboot	System will reboot.																			
data-exhausted	Data plan is exhausted.																			
session-disconnect	LTE data session is disconnected.																			
low-signal-strength	LTE signal strength is too low.																			
mode-switch	System is starting to use fallback OS image.																			
os-image-fallback	System networking mode switched.																			
fgt-backup-mode-switch	FortiGate backup work mode switched.																			
name	FortiExtender SMS notification receiver name.	string	Maximum length: 31																	
phone-number	Receiver phone number. Format: [+] [country code] [area code] [local phone number]. For example, +16501234567.	string	Maximum length: 31																	
status	SMS notification receiver status.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SMS notification receiver.</td></tr><tr><td>enable</td><td>Enable SMS notification receiver.</td></tr></table>	Option	Description	disable	Disable SMS notification receiver.	enable	Enable SMS notification receiver.													
Option	Description																			
disable	Disable SMS notification receiver.																			
enable	Enable SMS notification receiver.																			

config lan-extension

Parameter	Description	Type	Size	Default						
backhaul-interface	IPsec phase1 interface.	string	Maximum length: 15							
backhaul-ip	IPsec phase1 IPv4/FQDN. Used to specify the external IP/FQDN when the FortiGate unit is behind a NAT device.	string	Maximum length: 63							
ipsec-tunnel	IPsec tunnel name.	string	Maximum length: 15							
link-loadbalance	LAN extension link load balance strategy.	option	-	activebackup						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>activebackup</td><td>FortiExtender LAN extension active-backup.</td></tr><tr><td>loadbalance</td><td>FortiExtender LAN extension load-balance.</td></tr></table>				Option	Description	activebackup	FortiExtender LAN extension active-backup.	loadbalance	FortiExtender LAN extension load-balance.
Option	Description									
activebackup	FortiExtender LAN extension active-backup.									
loadbalance	FortiExtender LAN extension load-balance.									

config backhaul

Parameter	Description	Type	Size	Default
name	FortiExtender LAN extension backhaul name.	string	Maximum length: 31	
port	FortiExtender uplink port.	option	-	wan
	Option	Description		
	wan	FortiExtender WAN port.		
	lte1	FortiExtender LTE1 port.		
	lte2	FortiExtender LTE2 port.		
	port1	FortiExtender port1 port.		
	port2	FortiExtender port2 port.		
	port3	FortiExtender port3 port.		
	port4	FortiExtender port4 port.		
	port5	FortiExtender port5 port.		
	sfp	FortiExtender SFP port.		
role	FortiExtender uplink port.	option	-	primary

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>primary</i>	FortiExtender LAN extension primary role.		
	<i>secondary</i>	FortiExtender LAN extension secondary role.		
weight	WRR weight parameter.	integer	Minimum value: 1 Maximum value: 256	1

config downlinks

Parameter	Description	Type	Size	Default
name	FortiExtender LAN extension downlink config entry name.	string	Maximum length: 31	
port	FortiExtender LAN extension downlink port.	option	-	
	Option	Description		
	port1	FortiExtender port1 port.		
	port2	FortiExtender port2 port.		
	port3	FortiExtender port3 port.		
	port4	FortiExtender port4 port.		
	port5	FortiExtender port5 port.		
	lan1	FortiExtender LAN1 port.		
	lan2	FortiExtender LAN2 port.		
pvid	FortiExtender LAN extension downlink PVID.	integer	Minimum value: 0 Maximum value: 4089	0
type	FortiExtender LAN extension downlink type [port/vap].	option	-	port
	Option	Description		
	port	LAN extension Downlink type: port		
	vap	LAN extension Downlink type: Wi-Fi VAP		
vap	FortiExtender LAN extension downlink vap.	string	Maximum length: 31	

config traffic-split-services

Parameter	Description	Type	Size	Default
address	Address selection.	string	Maximum length: 79	
name	FortiExtender LAN extension tunnel split entry name.	string	Maximum length: 31	
service	Service selection.	string	Maximum length: 79	ALL
vsdb	Set video streaming traffic goes through local WAN [enable/disable].	option	-	disable
		Option	Description	
		<i>disable</i>	LAN extension traffice split disable	
		<i>enable</i>	LAN extension traffice split enable	

config wifi

Parameter	Description	Type	Size	Default
country	Country in which this FEX will operate (default = NA).	option	-	--
		Option	Description	
		--	NO_COUNTRY_SET	
		AF	AFGHANISTAN	
		AL	ALBANIA	
		DZ	ALGERIA	
		AS	AMERICAN SAMOA	
		AO	ANGOLA	
		AR	ARGENTINA	
		AM	ARMENIA	
		AU	AUSTRALIA	
		AT	AUSTRIA	
		AZ	AZERBAIJAN	
		BS	BAHAMAS	
		BH	BAHRAIN	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>BD</i>	BANGLADESH		
	<i>BB</i>	BARBADOS		
	<i>BY</i>	BELARUS		
	<i>BE</i>	BELGIUM		
	<i>BZ</i>	BELIZE		
	<i>BJ</i>	BENIN		
	<i>BM</i>	BERMUDA		
	<i>BT</i>	BHUTAN		
	<i>BO</i>	BOLIVIA		
	<i>BA</i>	BOSNIA AND HERZEGOVINA		
	<i>BW</i>	BOTSWANA		
	<i>BR</i>	BRAZIL		
	<i>BN</i>	BRUNEI DARUSSALAM		
	<i>BG</i>	BULGARIA		
	<i>BF</i>	BURKINA-FASO		
	<i>KH</i>	CAMBODIA		
	<i>CM</i>	CAMEROON		
	<i>KY</i>	CAYMAN ISLANDS		
	<i>CF</i>	CENTRAL AFRICA REPUBLIC		
	<i>TD</i>	CHAD		
	<i>CL</i>	CHILE		
	<i>CN</i>	CHINA		
	<i>CX</i>	CHRISTMAS ISLAND		
	<i>CO</i>	COLOMBIA		
	<i>CG</i>	CONGO REPUBLIC		
	<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO		
	<i>CR</i>	COSTA RICA		
	<i>HR</i>	CROATIA		
	<i>CY</i>	CYPRUS		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>CZ</i>	CZECH REPUBLIC		
	<i>DK</i>	DENMARK		
	<i>DJ</i>	DJIBOUTI		
	<i>DM</i>	DOMINICA		
	<i>DO</i>	DOMINICAN REPUBLIC		
	<i>EC</i>	ECUADOR		
	<i>EG</i>	EGYPT		
	<i>SV</i>	EL SALVADOR		
	<i>ET</i>	ETHIOPIA		
	<i>EE</i>	ESTONIA		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		
	<i>FO</i>	FAEROE ISLANDS		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GA</i>	GABON		
	<i>GE</i>	GEORGIA		
	<i>GM</i>	GAMBIA		
	<i>DE</i>	GERMANY		
	<i>GH</i>	GHANA		
	<i>GI</i>	GIBRALTAR		
	<i>GR</i>	GREECE		
	<i>GL</i>	GREENLAND		
	<i>GD</i>	GRENADA		
	<i>GP</i>	GUADELOUPE		
	<i>GU</i>	GUAM		
	<i>GT</i>	GUATEMALA		
	<i>GY</i>	GUYANA		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>HT</i>	HAITI		
	<i>HN</i>	HONDURAS		
	<i>HK</i>	HONG KONG		
	<i>HU</i>	HUNGARY		
	<i>IS</i>	ICELAND		
	<i>IN</i>	INDIA		
	<i>ID</i>	INDONESIA		
	<i>IQ</i>	IRAQ		
	<i>IE</i>	IRELAND		
	<i>IM</i>	ISLE OF MAN		
	<i>IL</i>	ISRAEL		
	<i>IT</i>	ITALY		
	<i>CI</i>	COTE_D_IVOIRE		
	<i>JM</i>	JAMAICA		
	<i>JO</i>	JORDAN		
	<i>KZ</i>	KAZAKHSTAN		
	<i>KE</i>	KENYA		
	<i>KR</i>	KOREA REPUBLIC		
	<i>KW</i>	KUWAIT		
	<i>LA</i>	LAOS		
	<i>LV</i>	LATVIA		
	<i>LB</i>	LEBANON		
	<i>LS</i>	LESOTHO		
	<i>LR</i>	LIBERIA		
	<i>LY</i>	LIBYA		
	<i>LI</i>	LIECHTENSTEIN		
	<i>LT</i>	LITHUANIA		
	<i>LU</i>	LUXEMBOURG		
	<i>MO</i>	MACAU SAR		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>MK</i>	MACEDONIA, FYRO		
	<i>MG</i>	MADAGASCAR		
	<i>MW</i>	MALAWI		
	<i>MY</i>	MALAYSIA		
	<i>MV</i>	MALDIVES		
	<i>ML</i>	MALI		
	<i>MT</i>	MALTA		
	<i>MH</i>	MARSHALL ISLANDS		
	<i>MQ</i>	MARTINIQUE		
	<i>MR</i>	MAURITANIA		
	<i>MU</i>	MAURITIUS		
	<i>YT</i>	MAYOTTE		
	<i>MX</i>	MEXICO		
	<i>FM</i>	MICRONESIA		
	<i>MD</i>	REPUBLIC OF MOLDOVA		
	<i>MC</i>	MONACO		
	<i>MN</i>	MONGOLIA		
	<i>MA</i>	MOROCCO		
	<i>MZ</i>	MOZAMBIQUE		
	<i>MM</i>	MYANMAR		
	<i>NA</i>	NAMIBIA		
	<i>NP</i>	NEPAL		
	<i>NL</i>	NETHERLANDS		
	<i>AN</i>	NETHERLANDS ANTILLES		
	<i>AW</i>	ARUBA		
	<i>NZ</i>	NEW ZEALAND		
	<i>NI</i>	NICARAGUA		
	<i>NE</i>	NIGER		
	<i>NG</i>	NIGERIA		

Parameter	Description	Type	Size	Default

Option	Description
<i>NO</i>	NORWAY
<i>MP</i>	NORTHERN MARIANA ISLANDS
<i>OM</i>	OMAN
<i>PK</i>	PAKISTAN
<i>PW</i>	PALAU
<i>PA</i>	PANAMA
<i>PG</i>	PAPUA NEW GUINEA
<i>PY</i>	PARAGUAY
<i>PE</i>	PERU
<i>PH</i>	PHILIPPINES
<i>PL</i>	POLAND
<i>PT</i>	PORTUGAL
<i>PR</i>	PUERTO RICO
<i>QA</i>	QATAR
<i>RE</i>	REUNION
<i>RO</i>	ROMANIA
<i>RU</i>	RUSSIA
<i>RW</i>	RWANDA
<i>BL</i>	SAINT BARTHELEMY
<i>KN</i>	SAINT KITTS AND NEVIS
<i>LC</i>	SAINT LUCIA
<i>MF</i>	SAINT MARTIN
<i>PM</i>	SAINT PIERRE AND MIQUELON
<i>VC</i>	SAINT VINCENT AND GRENADIENS
<i>SA</i>	SAUDI ARABIA
<i>SN</i>	SENEGAL
<i>RS</i>	REPUBLIC OF SERBIA
<i>ME</i>	MONTENEGRO
<i>SL</i>	SIERRA LEONE

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>SG</i>	SINGAPORE		
	<i>SK</i>	SLOVAKIA		
	<i>SI</i>	SLOVENIA		
	<i>SO</i>	SOMALIA		
	<i>ZA</i>	SOUTH AFRICA		
	<i>ES</i>	SPAIN		
	<i>LK</i>	SRI LANKA		
	<i>SR</i>	SURINAME		
	<i>SZ</i>	SWAZILAND		
	<i>SE</i>	SWEDEN		
	<i>CH</i>	SWITZERLAND		
	<i>TW</i>	TAIWAN		
	<i>TZ</i>	TANZANIA		
	<i>TH</i>	THAILAND		
	<i>TL</i>	TIMOR-LESTE		
	<i>TG</i>	TOGO		
	<i>TT</i>	TRINIDAD AND TOBAGO		
	<i>TN</i>	TUNISIA		
	<i>TR</i>	TURKEY		
	<i>TM</i>	TURKMENISTAN		
	<i>AE</i>	UNITED ARAB EMIRATES		
	<i>TC</i>	TURKS AND CAICOS		
	<i>UG</i>	UGANDA		
	<i>UA</i>	UKRAINE		
	<i>GB</i>	UNITED KINGDOM		
	<i>US</i>	UNITED STATES2		
	<i>PS</i>	UNITED STATES (PUBLIC SAFETY)		
	<i>UY</i>	URUGUAY		
	<i>UZ</i>	UZBEKISTAN		

Parameter	Description	Type	Size	Default
	Option	Description		
	VU	VANUATU		
	VE	VENEZUELA		
	VN	VIET NAM		
	VI	VIRGIN ISLANDS		
	WF	WALLIS AND FUTUNA		
	YE	YEMEN		
	ZM	ZAMBIA		
	ZW	ZIMBABWE		
	JP	JAPAN14		
	CA	CANADA2		

config radio-1

Parameter	Description	Type	Size	Default
80211d	Enable/disable Wi-Fi 802.11d.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable 802.11d.		
	<i>enable</i>	Enable 802.11d.		
band	Wi-Fi band selection 2.4GHz / 5GHz.	option	-	2.4GHz
	Option	Description		
	<i>2.4GHz</i>	Wi-Fi 2.4GHz		
bandwidth	Wi-Fi channel bandwidth.	option	-	auto
	Option	Description		
	<i>auto</i>	Wi-Fi channel bandwidth auto		
	<i>20MHz</i>	Wi-Fi channel bandwidth 20MHz		
	<i>40MHz</i>	Wi-Fi channel bandwidth 40MHz		
	<i>80MHz</i>	Wi-Fi channel bandwidth 80MHz		

Parameter	Description	Type	Size	Default
beacon-interval	Wi-Fi beacon interval in milliseconds (100 - 3500, default = 100).	integer	Minimum value: 100 Maximum value: 3500	100
bss-color	Wi-Fi 802.11AX BSS color value (0 - 63, 0 = disable, default = 0).	integer	Minimum value: 0 Maximum value: 63	0
bss-color-mode	Wi-Fi 802.11AX BSS color mode.	option	-	auto
	Option	Description		
	auto	Wi-Fi BSS color mode auto		
	static	Wi-Fi BSS color mode static		
channel	Wi-Fi channels.	option	-	
	Option	Description		
	CH1	Channel 1		
	CH2	Channel 2		
	CH3	Channel 3		
	CH4	Channel 4		
	CH5	Channel 5		
	CH6	Channel 6		
	CH7	Channel 7		
	CH8	Channel 8		
	CH9	Channel 9		
	CH10	Channel 10		
CH11	Channel 11			
extension-channel	Wi-Fi extension channel.	option	-	auto
	Option	Description		
	auto	Wi-Fi extension channel auto.		
	higher	Wi-Fi extension channel higher.		
	lower	Wi-Fi extension channel lower.		

Parameter	Description	Type	Size	Default																				
guard-interval	Wi-Fi guard interval.	option	-	auto																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Wi-Fi guard_interval auto</td></tr><tr><td>400ns</td><td>Wi-Fi guard_interval 400ns</td></tr><tr><td>800ns</td><td>Wi-Fi guard_interval 800ns</td></tr></table>	Option	Description	auto	Wi-Fi guard_interval auto	400ns	Wi-Fi guard_interval 400ns	800ns	Wi-Fi guard_interval 800ns															
	Option	Description																						
	auto	Wi-Fi guard_interval auto																						
	400ns	Wi-Fi guard_interval 400ns																						
800ns	Wi-Fi guard_interval 800ns																							
lan-ext-vap	Wi-Fi LAN-Extention VAP. Select only one VAP.	string	Maximum length: 31																					
local-vaps <name>	Wi-Fi local VAP. Select up to three VAPs. Wi-Fi local VAP name.	string	Maximum length: 79																					
max-clients	Maximum number of Wi-Fi radio clients (0 - 512, 0 = unlimited, default = 0).	integer	Minimum value: 0 Maximum value: 512	0																				
mode	Wi-Fi radio mode AP(LAN mode) / Client(WAN mode).	option	-	AP																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>AP</td><td>AP Mode (LAN mode)</td></tr><tr><td>Client</td><td>Client mode (WAN mode)</td></tr></table>	Option	Description	AP	AP Mode (LAN mode)	Client	Client mode (WAN mode)																	
	Option	Description																						
	AP	AP Mode (LAN mode)																						
Client	Client mode (WAN mode)																							
operating-standard	Wi-Fi operating standard.	option	-	auto																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Wi-Fi operating standard auto</td></tr><tr><td>11A-N-AC-AX</td><td>Wi-Fi support 802.11 A-N-AC</td></tr><tr><td>11A-N-AC</td><td>Wi-Fi support 802.11 A-N-AC</td></tr><tr><td>11A-N</td><td>Wi-Fi support 802.11 A-N</td></tr><tr><td>11A</td><td>Wi-Fi support 802.11 A</td></tr><tr><td>11N-AC-AX</td><td>Wi-Fi support 802.11 N-AC-AX</td></tr><tr><td>11AC-AX</td><td>Wi-Fi support 802.11 AC-AX</td></tr><tr><td>11AC</td><td>Wi-Fi support 802.11 AC</td></tr><tr><td>11N-AC</td><td>Wi-Fi support 802.11 N-AC</td></tr></table>	Option	Description	auto	Wi-Fi operating standard auto	11A-N-AC-AX	Wi-Fi support 802.11 A-N-AC	11A-N-AC	Wi-Fi support 802.11 A-N-AC	11A-N	Wi-Fi support 802.11 A-N	11A	Wi-Fi support 802.11 A	11N-AC-AX	Wi-Fi support 802.11 N-AC-AX	11AC-AX	Wi-Fi support 802.11 AC-AX	11AC	Wi-Fi support 802.11 AC	11N-AC	Wi-Fi support 802.11 N-AC			
	Option	Description																						
	auto	Wi-Fi operating standard auto																						
	11A-N-AC-AX	Wi-Fi support 802.11 A-N-AC																						
	11A-N-AC	Wi-Fi support 802.11 A-N-AC																						
	11A-N	Wi-Fi support 802.11 A-N																						
	11A	Wi-Fi support 802.11 A																						
	11N-AC-AX	Wi-Fi support 802.11 N-AC-AX																						
	11AC-AX	Wi-Fi support 802.11 AC-AX																						
11AC	Wi-Fi support 802.11 AC																							
11N-AC	Wi-Fi support 802.11 N-AC																							

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>11B-G-N-AX</td><td>Wi-Fi support 802.11 B-G-N-AX</td></tr><tr><td>11B-G-N</td><td>Wi-Fi support 802.11 B-G-N</td></tr><tr><td>11B-G</td><td>Wi-Fi support 802.11 B-G</td></tr><tr><td>11B</td><td>Wi-Fi support 802.11 B</td></tr><tr><td>11G-N-AX</td><td>Wi-Fi support 802.11 G-N-AX</td></tr><tr><td>11N-AX</td><td>Wi-Fi support 802.11 N-AX</td></tr><tr><td>11AX</td><td>Wi-Fi support 802.11 AX</td></tr><tr><td>11G-N</td><td>Wi-Fi support 802.11 G-N</td></tr><tr><td>11N</td><td>Wi-Fi support 802.11 N</td></tr><tr><td>11G</td><td>Wi-Fi support 802.11 G</td></tr></table>	Option	Description	11B-G-N-AX	Wi-Fi support 802.11 B-G-N-AX	11B-G-N	Wi-Fi support 802.11 B-G-N	11B-G	Wi-Fi support 802.11 B-G	11B	Wi-Fi support 802.11 B	11G-N-AX	Wi-Fi support 802.11 G-N-AX	11N-AX	Wi-Fi support 802.11 N-AX	11AX	Wi-Fi support 802.11 AX	11G-N	Wi-Fi support 802.11 G-N	11N	Wi-Fi support 802.11 N	11G	Wi-Fi support 802.11 G			
	Option	Description																								
	11B-G-N-AX	Wi-Fi support 802.11 B-G-N-AX																								
	11B-G-N	Wi-Fi support 802.11 B-G-N																								
	11B-G	Wi-Fi support 802.11 B-G																								
	11B	Wi-Fi support 802.11 B																								
	11G-N-AX	Wi-Fi support 802.11 G-N-AX																								
	11N-AX	Wi-Fi support 802.11 N-AX																								
	11AX	Wi-Fi support 802.11 AX																								
	11G-N	Wi-Fi support 802.11 G-N																								
	11N	Wi-Fi support 802.11 N																								
11G	Wi-Fi support 802.11 G																									
power-level	Wi-Fi power level in percent (0 - 100, 0 = auto, default = 100).	integer	Minimum value: 0 Maximum value: 100	100																						
status	Enable/disable Wi-Fi radio.	option	-	disable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Wi-Fi radio.</td></tr><tr><td>enable</td><td>Enable Wi-Fi radio.</td></tr></table>	Option	Description	disable	Disable Wi-Fi radio.	enable	Enable Wi-Fi radio.																			
	Option	Description																								
	disable	Disable Wi-Fi radio.																								
enable	Enable Wi-Fi radio.																									

config radio-2

Parameter	Description	Type	Size	Default						
80211d	Enable/disable Wi-Fi 802.11d.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable 802.11d.</td></tr><tr><td>enable</td><td>Enable 802.11d.</td></tr></table>	Option	Description	disable	Disable 802.11d.	enable	Enable 802.11d.			
Option	Description									
disable	Disable 802.11d.									
enable	Enable 802.11d.									
band	Wi-Fi band selection 2.4GHz / 5GHz.	option	-	5GHz						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5GHz</td><td>Wi-Fi 5GHz</td></tr></table>	Option	Description	5GHz	Wi-Fi 5GHz					
Option	Description									
5GHz	Wi-Fi 5GHz									
bandwidth	Wi-Fi channel bandwidth.	option	-	auto						

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Wi-Fi channel bandwidth auto</td></tr><tr><td>20MHz</td><td>Wi-Fi channel bandwidth 20MHz</td></tr><tr><td>40MHz</td><td>Wi-Fi channel bandwidth 40MHz</td></tr><tr><td>80MHz</td><td>Wi-Fi channel bandwidth 80MHz</td></tr></table>	Option	Description	auto	Wi-Fi channel bandwidth auto	20MHz	Wi-Fi channel bandwidth 20MHz	40MHz	Wi-Fi channel bandwidth 40MHz	80MHz	Wi-Fi channel bandwidth 80MHz																	
	Option	Description																										
	auto	Wi-Fi channel bandwidth auto																										
	20MHz	Wi-Fi channel bandwidth 20MHz																										
	40MHz	Wi-Fi channel bandwidth 40MHz																										
80MHz	Wi-Fi channel bandwidth 80MHz																											
beacon-interval	Wi-Fi beacon interval in milliseconds (100 - 3500, default = 100).	integer	Minimum value: 100 Maximum value: 3500	100																								
bss-color	Wi-Fi 802.11AX BSS color value (0 - 63, 0 = disable, default = 0).	integer	Minimum value: 0 Maximum value: 63	0																								
bss-color-mode	Wi-Fi 802.11AX BSS color mode.	option	-	auto																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Wi-Fi BSS color mode auto</td></tr><tr><td>static</td><td>Wi-Fi BSS color mode static</td></tr></table>	Option	Description	auto	Wi-Fi BSS color mode auto	static	Wi-Fi BSS color mode static																					
	Option	Description																										
	auto	Wi-Fi BSS color mode auto																										
static	Wi-Fi BSS color mode static																											
channel	Wi-Fi channels.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>CH36</td><td>Channel 36</td></tr><tr><td>CH40</td><td>Channel 40</td></tr><tr><td>CH44</td><td>Channel 44</td></tr><tr><td>CH48</td><td>Channel 48</td></tr><tr><td>CH52</td><td>Channel 52</td></tr><tr><td>CH56</td><td>Channel 56</td></tr><tr><td>CH60</td><td>Channel 60</td></tr><tr><td>CH64</td><td>Channel 64</td></tr><tr><td>CH100</td><td>Channel 100</td></tr><tr><td>CH104</td><td>Channel 104</td></tr><tr><td>CH108</td><td>Channel 108</td></tr></table>	Option	Description	CH36	Channel 36	CH40	Channel 40	CH44	Channel 44	CH48	Channel 48	CH52	Channel 52	CH56	Channel 56	CH60	Channel 60	CH64	Channel 64	CH100	Channel 100	CH104	Channel 104	CH108	Channel 108			
	Option	Description																										
	CH36	Channel 36																										
	CH40	Channel 40																										
	CH44	Channel 44																										
	CH48	Channel 48																										
	CH52	Channel 52																										
	CH56	Channel 56																										
	CH60	Channel 60																										
	CH64	Channel 64																										
	CH100	Channel 100																										
	CH104	Channel 104																										
	CH108	Channel 108																										

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>CH112</td><td>Channel 112</td></tr><tr><td>CH116</td><td>Channel 116</td></tr><tr><td>CH120</td><td>Channel 120</td></tr><tr><td>CH124</td><td>Channel 124</td></tr><tr><td>CH128</td><td>Channel 128</td></tr><tr><td>CH132</td><td>Channel 132</td></tr><tr><td>CH136</td><td>Channel 136</td></tr><tr><td>CH140</td><td>Channel 140</td></tr><tr><td>CH144</td><td>Channel 144</td></tr><tr><td>CH149</td><td>Channel 149</td></tr><tr><td>CH153</td><td>Channel 153</td></tr><tr><td>CH157</td><td>Channel 157</td></tr><tr><td>CH161</td><td>Channel 161</td></tr><tr><td>CH165</td><td>Channel 165</td></tr></table>	Option	Description	CH112	Channel 112	CH116	Channel 116	CH120	Channel 120	CH124	Channel 124	CH128	Channel 128	CH132	Channel 132	CH136	Channel 136	CH140	Channel 140	CH144	Channel 144	CH149	Channel 149	CH153	Channel 153	CH157	Channel 157	CH161	Channel 161	CH165	Channel 165			
	Option	Description																																
	CH112	Channel 112																																
	CH116	Channel 116																																
	CH120	Channel 120																																
	CH124	Channel 124																																
	CH128	Channel 128																																
	CH132	Channel 132																																
	CH136	Channel 136																																
	CH140	Channel 140																																
	CH144	Channel 144																																
	CH149	Channel 149																																
	CH153	Channel 153																																
	CH157	Channel 157																																
	CH161	Channel 161																																
	CH165	Channel 165																																
extension-channel	Wi-Fi extension channel.	option	-	auto																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Wi-Fi extension channel auto.</td></tr><tr><td>higher</td><td>Wi-Fi extension channel higher.</td></tr><tr><td>lower</td><td>Wi-Fi extension channel lower.</td></tr></table>	Option	Description	auto	Wi-Fi extension channel auto.	higher	Wi-Fi extension channel higher.	lower	Wi-Fi extension channel lower.																									
	Option	Description																																
	auto	Wi-Fi extension channel auto.																																
	higher	Wi-Fi extension channel higher.																																
lower	Wi-Fi extension channel lower.																																	
guard-interval	Wi-Fi guard interval.	option	-	auto																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Wi-Fi guard_interval auto</td></tr><tr><td>400ns</td><td>Wi-Fi guard_interval 400ns</td></tr><tr><td>800ns</td><td>Wi-Fi guard_interval 800ns</td></tr></table>	Option	Description	auto	Wi-Fi guard_interval auto	400ns	Wi-Fi guard_interval 400ns	800ns	Wi-Fi guard_interval 800ns																									
	Option	Description																																
	auto	Wi-Fi guard_interval auto																																
	400ns	Wi-Fi guard_interval 400ns																																
800ns	Wi-Fi guard_interval 800ns																																	
lan-ext-vap	Wi-Fi LAN-Extention VAP. Select only one VAP.	string	Maximum length: 31																															
local-vaps <name>	Wi-Fi local VAP. Select up to three VAPs. Wi-Fi local VAP name.	string	Maximum length: 79																															

Parameter	Description	Type	Size	Default																																								
max-clients	Maximum number of Wi-Fi radio clients (0 - 512, 0 = unlimited, default = 0).	integer	Minimum value: 0 Maximum value: 512	0																																								
mode	Wi-Fi radio mode AP(LAN mode) / Client(WAN mode).	option	-	AP																																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>AP</td><td>AP Mode (LAN mode)</td></tr><tr><td>Client</td><td>Client mode (WAN mode)</td></tr></table>	Option	Description	AP	AP Mode (LAN mode)	Client	Client mode (WAN mode)																																					
Option	Description																																											
AP	AP Mode (LAN mode)																																											
Client	Client mode (WAN mode)																																											
operating-standard	Wi-Fi operating standard.	option	-	auto																																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Wi-Fi operating standard auto</td></tr><tr><td>11A-N-AC-AX</td><td>Wi-Fi support 802.11 A-N-AC</td></tr><tr><td>11A-N-AC</td><td>Wi-Fi support 802.11 A-N-AC</td></tr><tr><td>11A-N</td><td>Wi-Fi support 802.11 A-N</td></tr><tr><td>11A</td><td>Wi-Fi support 802.11 A</td></tr><tr><td>11N-AC-AX</td><td>Wi-Fi support 802.11 N-AC-AX</td></tr><tr><td>11AC-AX</td><td>Wi-Fi support 802.11 AC-AX</td></tr><tr><td>11AC</td><td>Wi-Fi support 802.11 AC</td></tr><tr><td>11N-AC</td><td>Wi-Fi support 802.11 N-AC</td></tr><tr><td>11B-G-N-AX</td><td>Wi-Fi support 802.11 B-G-N-AX</td></tr><tr><td>11B-G-N</td><td>Wi-Fi support 802.11 B-G-N</td></tr><tr><td>11B-G</td><td>Wi-Fi support 802.11 B-G</td></tr><tr><td>11B</td><td>Wi-Fi support 802.11 B</td></tr><tr><td>11G-N-AX</td><td>Wi-Fi support 802.11 G-N-AX</td></tr><tr><td>11N-AX</td><td>Wi-Fi support 802.11 N-AX</td></tr><tr><td>11AX</td><td>Wi-Fi support 802.11 AX</td></tr><tr><td>11G-N</td><td>Wi-Fi support 802.11 G-N</td></tr><tr><td>11N</td><td>Wi-Fi support 802.11 N</td></tr><tr><td>11G</td><td>Wi-Fi support 802.11 G</td></tr></table>	Option	Description	auto	Wi-Fi operating standard auto	11A-N-AC-AX	Wi-Fi support 802.11 A-N-AC	11A-N-AC	Wi-Fi support 802.11 A-N-AC	11A-N	Wi-Fi support 802.11 A-N	11A	Wi-Fi support 802.11 A	11N-AC-AX	Wi-Fi support 802.11 N-AC-AX	11AC-AX	Wi-Fi support 802.11 AC-AX	11AC	Wi-Fi support 802.11 AC	11N-AC	Wi-Fi support 802.11 N-AC	11B-G-N-AX	Wi-Fi support 802.11 B-G-N-AX	11B-G-N	Wi-Fi support 802.11 B-G-N	11B-G	Wi-Fi support 802.11 B-G	11B	Wi-Fi support 802.11 B	11G-N-AX	Wi-Fi support 802.11 G-N-AX	11N-AX	Wi-Fi support 802.11 N-AX	11AX	Wi-Fi support 802.11 AX	11G-N	Wi-Fi support 802.11 G-N	11N	Wi-Fi support 802.11 N	11G	Wi-Fi support 802.11 G			
Option	Description																																											
auto	Wi-Fi operating standard auto																																											
11A-N-AC-AX	Wi-Fi support 802.11 A-N-AC																																											
11A-N-AC	Wi-Fi support 802.11 A-N-AC																																											
11A-N	Wi-Fi support 802.11 A-N																																											
11A	Wi-Fi support 802.11 A																																											
11N-AC-AX	Wi-Fi support 802.11 N-AC-AX																																											
11AC-AX	Wi-Fi support 802.11 AC-AX																																											
11AC	Wi-Fi support 802.11 AC																																											
11N-AC	Wi-Fi support 802.11 N-AC																																											
11B-G-N-AX	Wi-Fi support 802.11 B-G-N-AX																																											
11B-G-N	Wi-Fi support 802.11 B-G-N																																											
11B-G	Wi-Fi support 802.11 B-G																																											
11B	Wi-Fi support 802.11 B																																											
11G-N-AX	Wi-Fi support 802.11 G-N-AX																																											
11N-AX	Wi-Fi support 802.11 N-AX																																											
11AX	Wi-Fi support 802.11 AX																																											
11G-N	Wi-Fi support 802.11 G-N																																											
11N	Wi-Fi support 802.11 N																																											
11G	Wi-Fi support 802.11 G																																											

Parameter	Description	Type	Size	Default						
power-level	Wi-Fi power level in percent (0 - 100, 0 = auto, default = 100).	integer	Minimum value: 0 Maximum value: 100	100						
status	Enable/disable Wi-Fi radio.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Wi-Fi radio.</td></tr><tr><td><i>enable</i></td><td>Enable Wi-Fi radio.</td></tr></table>				Option	Description	<i>disable</i>	Disable Wi-Fi radio.	<i>enable</i>	Enable Wi-Fi radio.
Option	Description									
<i>disable</i>	Disable Wi-Fi radio.									
<i>enable</i>	Enable Wi-Fi radio.									

config extension-controller extender-vap

FortiExtender wifi vap configuration.

```

config extension-controller extender-vap
  Description: FortiExtender wifi vap configuration.
  edit <name>
    set allowaccess {option1}, {option2}, ...
    set auth-server-address {string}
    set auth-server-port {integer}
    set auth-server-secret {string}
    set broadcast-ssid [disable|enable]
    set bss-color-partial [disable|enable]
    set dtim {integer}
    set end-ip {ipv4-address}
    set ip-address {ipv4-classnet-host}
    set max-clients {integer}
    set mu-mimo [disable|enable]
    set passphrase {password}
    set pmf [disabled|optional|...]
    set rts-threshold {integer}
    set sae-password {password}
    set security [OPEN|WPA2-Personal|...]
    set ssid {string}
    set start-ip {ipv4-address}
    set target-wake-time [disable|enable]
    set type [local-vap|lan-ext-vap]
  next
end

```

config extension-controller extender-vap

Parameter	Description	Type	Size	Default														
allowaccess	Control management access to the managed extender. Separate entries with a space.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING access.</td></tr><tr><td>telnet</td><td>TELNET access.</td></tr><tr><td>http</td><td>HTTP access.</td></tr><tr><td>https</td><td>HTTPS access.</td></tr><tr><td>ssh</td><td>SSH access.</td></tr><tr><td>snmp</td><td>SNMP access.</td></tr></table>	Option	Description	ping	PING access.	telnet	TELNET access.	http	HTTP access.	https	HTTPS access.	ssh	SSH access.	snmp	SNMP access.			
Option	Description																	
ping	PING access.																	
telnet	TELNET access.																	
http	HTTP access.																	
https	HTTPS access.																	
ssh	SSH access.																	
snmp	SNMP access.																	
auth-server-address	Wi-Fi Authentication Server Address (IPv4 format).	string	Maximum length: 63															
auth-server-port	Wi-Fi Authentication Server Port.	integer	Minimum value: 1 Maximum value: 65535	0														
auth-server-secret	Wi-Fi Authentication Server Secret.	string	Maximum length: 63															
broadcast-ssid	Wi-Fi broadcast SSID enable / disable.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable broadcast SSID.</td></tr><tr><td>enable</td><td>Enable broadcast SSID.</td></tr></table>	Option	Description	disable	Disable broadcast SSID.	enable	Enable broadcast SSID.											
Option	Description																	
disable	Disable broadcast SSID.																	
enable	Enable broadcast SSID.																	
bss-color-partial	Wi-Fi 802.11AX bss color partial enable / disable, default = enable.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable bss color partial.</td></tr><tr><td>enable</td><td>Enable bss color partial.</td></tr></table>	Option	Description	disable	Disable bss color partial.	enable	Enable bss color partial.											
Option	Description																	
disable	Disable bss color partial.																	
enable	Enable bss color partial.																	
dtim	Wi-Fi DTIM (1 - 255) default = 1.	integer	Minimum value: 1 Maximum value: 255	1														

Parameter	Description	Type	Size	Default								
end-ip	End ip address.	ipv4-address	Not Specified	0.0.0.0								
ip-address	Extender ip address.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								
max-clients	Wi-Fi max clients (0 - 512), default = 0 (no limit)	integer	Minimum value: 0 Maximum value: 512	0								
mu-mimo	Wi-Fi multi-user MIMO enable / disable, default = enable.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable multi-user MIMO.</td></tr><tr><td>enable</td><td>Enable multi-user MIMO.</td></tr></table>				Option	Description	disable	Disable multi-user MIMO.	enable	Enable multi-user MIMO.		
	Option	Description										
	disable	Disable multi-user MIMO.										
enable	Enable multi-user MIMO.											
name	Wi-Fi VAP name.	string	Maximum length: 15									
passphrase	Wi-Fi passphrase.	password	Not Specified									
pmf	Wi-Fi pmf enable/disable, default = disable.	option	-	disabled								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disabled</td><td>Disable PMF (Protected Management Frames).</td></tr><tr><td>optional</td><td>Set PMF (Protected Management Frames) optional.</td></tr><tr><td>required</td><td>Require PMF (Protected Management Frames).</td></tr></table>				Option	Description	disabled	Disable PMF (Protected Management Frames).	optional	Set PMF (Protected Management Frames) optional.	required	Require PMF (Protected Management Frames).
	Option	Description										
	disabled	Disable PMF (Protected Management Frames).										
	optional	Set PMF (Protected Management Frames) optional.										
required	Require PMF (Protected Management Frames).											
rts-threshold	Wi-Fi RTS Threshold (256 - 2347), default = 2347 (RTS/CTS disabled).	integer	Minimum value: 256 Maximum value: 2347	2347								
sae-password	Wi-Fi SAE Password.	password	Not Specified									
security	Wi-Fi security.	option	-	WPA2-Personal								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>OPEN</td><td>Wi-Fi security OPEN</td></tr></table>				Option	Description	OPEN	Wi-Fi security OPEN				
	Option	Description										
OPEN	Wi-Fi security OPEN											

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>WPA2-Personal</td><td>Wi-Fi security WPA2 Personal</td></tr><tr><td>WPA-WPA2-Personal</td><td>Wi-Fi security WPA-WPA2 Personal</td></tr><tr><td>WPA3-SAE</td><td>Wi-Fi security WPA3 SAE</td></tr><tr><td>WPA3-SAE-Transition</td><td>Wi-Fi security WPA3 SAE Transition</td></tr><tr><td>WPA2-Enterprise</td><td>Wi-Fi security WPA2 Enterprise</td></tr><tr><td>WPA3-Enterprise-only</td><td>Wi-Fi security WPA3 Enterprise only</td></tr><tr><td>WPA3-Enterprise-transition</td><td>Wi-Fi security WPA3 Enterprise Transition</td></tr><tr><td>WPA3-Enterprise-192-bit</td><td>Wi-Fi security WPA3 Enterprise 192-bit</td></tr></table>	Option	Description	WPA2-Personal	Wi-Fi security WPA2 Personal	WPA-WPA2-Personal	Wi-Fi security WPA-WPA2 Personal	WPA3-SAE	Wi-Fi security WPA3 SAE	WPA3-SAE-Transition	Wi-Fi security WPA3 SAE Transition	WPA2-Enterprise	Wi-Fi security WPA2 Enterprise	WPA3-Enterprise-only	Wi-Fi security WPA3 Enterprise only	WPA3-Enterprise-transition	Wi-Fi security WPA3 Enterprise Transition	WPA3-Enterprise-192-bit	Wi-Fi security WPA3 Enterprise 192-bit			
	Option	Description																				
	WPA2-Personal	Wi-Fi security WPA2 Personal																				
	WPA-WPA2-Personal	Wi-Fi security WPA-WPA2 Personal																				
	WPA3-SAE	Wi-Fi security WPA3 SAE																				
	WPA3-SAE-Transition	Wi-Fi security WPA3 SAE Transition																				
	WPA2-Enterprise	Wi-Fi security WPA2 Enterprise																				
	WPA3-Enterprise-only	Wi-Fi security WPA3 Enterprise only																				
	WPA3-Enterprise-transition	Wi-Fi security WPA3 Enterprise Transition																				
WPA3-Enterprise-192-bit	Wi-Fi security WPA3 Enterprise 192-bit																					
ssid	Wi-Fi SSID.	string	Maximum length: 32																			
start-ip	Start ip address.	ipv4-address	Not Specified	0.0.0.0																		
target-wake-time	Wi-Fi 802.11AX target wake time enable / disable, default = enable.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable target wake time.</td></tr><tr><td>enable</td><td>Enable target wake time.</td></tr></table>	Option	Description	disable	Disable target wake time.	enable	Enable target wake time.															
	Option	Description																				
	disable	Disable target wake time.																				
enable	Enable target wake time.																					
type	Wi-Fi VAP type local-vap / lan-extension-vap.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>local-vap</td><td>Local VAP.</td></tr><tr><td>lan-ext-vap</td><td>Lan Extension VAP.</td></tr></table>	Option	Description	local-vap	Local VAP.	lan-ext-vap	Lan Extension VAP.															
	Option	Description																				
	local-vap	Local VAP.																				
lan-ext-vap	Lan Extension VAP.																					

config extension-controller fortigate

FortiGate controller configuration.


```

config extension-controller fortigate
  Description: FortiGate controller configuration.
  edit <name>
    set authorized [discovered|disable|...]
    set description {string}
    set device-id {integer}
    set hostname {string}
    set id {string}
    set profile {string}
    set vdom {integer}
  next
end

```

config extension-controller fortigate

Parameter	Description	Type	Size	Default
authorized	Enable/disable FortiGate administration.	option	-	discovered
	Option	Description		
	<i>discovered</i>	Controller discovered this FortiGate.		
	<i>disable</i>	Controller is configured to not provide service to this FortiGate.		
	<i>enable</i>	Controller is configured to provide service to this FortiGate.		
description	Description.	string	Maximum length: 255	
device-id	Device ID.	integer	Minimum value: 1026 0 Maximum value: 4294967295	
hostname	FortiGate hostname.	string	Maximum length: 31	
id	FortiGate serial number.	string	Maximum length: 19	
name	FortiGate entry name.	string	Maximum length: 19	
profile	FortiGate profile configuration.	string	Maximum length: 31	
vdom	VDOM. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config extension-controller fortigate-profile

FortiGate connector profile configuration.

```
config extension-controller fortigate-profile
  Description: FortiGate connector profile configuration.
  edit <name>
    set extension {option}
    set id {integer}
    config lan-extension
      Description: FortiGate connector LAN extension configuration.
      set backhaul-interface {string}
      set backhaul-ip {string}
      set ipsec-tunnel {string}
    end
  next
end
```

config extension-controller fortigate-profile

Parameter	Description	Type	Size	Default
extension	Extension option. Read-only.	option	-	lan-extension
	Option	Description		
	lan-extension	LAN extension.		
id	ID.	integer	Minimum value: 0 Maximum value: 102400000	32
name	FortiGate connector profile name.	string	Maximum length: 31	

config lan-extension

Parameter	Description	Type	Size	Default
backhaul-interface	IPsec phase1 interface.	string	Maximum length: 15	
backhaul-ip	IPsec phase1 IPv4/FQDN. Used to specify the external IP/FQDN when the FortiGate unit is behind a NAT device.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
ipsec-tunnel	IPsec tunnel name.	string	Maximum length: 15	

file-filter

This section includes syntax for the following commands:

- [config file-filter profile on page 340](#)

config file-filter profile

Configure file-filter profiles.

```
config file-filter profile
  Description: Configure file-filter profiles.
  edit <name>
    set comment {var-string}
    set extended-log [disable|enable]
    set feature-set [flow|proxy]
    set log [disable|enable]
    set replacemsg-group {string}
    config rules
      Description: File filter rules.
      edit <name>
        set action [log-only|block]
        set comment {var-string}
        set direction [incoming|outgoing|...]
        set file-type <name1>, <name2>, ...
        set password-protected [yes|any]
        set protocol {option1}, {option2}, ...
      next
    end
    set scan-archive-contents [disable|enable]
  next
end
```

config file-filter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
extended-log	Enable/disable file-filter extended logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable extended logging.		
	<i>enable</i>	Enable extended logging.		
feature-set	Flow/proxy feature set.	option	-	flow
	Option	Description		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
log	Enable/disable file-filter logging.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
name	Profile name.	string	Maximum length: 47	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
scan-archive-contents	Enable/disable archive contents scan.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable scanning archive contents.		
	<i>enable</i>	Enable scanning archive contents.		

config rules

Parameter	Description	Type	Size	Default
action	Action taken for matched file.	option	-	log-only
	Option	Description		
	<i>log-only</i>	Allow the content and write a log message.		
	<i>block</i>	Block the content and write a log message.		
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default																		
direction	Traffic direction (HTTP, FTP, SSH, CIFS, and MAPI only).	option	-	any																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>incoming</i></td><td>Match files transmitted in the session's reply direction.</td></tr><tr><td><i>outgoing</i></td><td>Match files transmitted in the session's originating direction.</td></tr><tr><td><i>any</i></td><td>Match files transmitted in the session's originating and reply directions.</td></tr></table>	Option	Description	<i>incoming</i>	Match files transmitted in the session's reply direction.	<i>outgoing</i>	Match files transmitted in the session's originating direction.	<i>any</i>	Match files transmitted in the session's originating and reply directions.													
Option	Description																					
<i>incoming</i>	Match files transmitted in the session's reply direction.																					
<i>outgoing</i>	Match files transmitted in the session's originating direction.																					
<i>any</i>	Match files transmitted in the session's originating and reply directions.																					
file-type <name>	Select file type. File type name.	string	Maximum length: 39																			
name	File-filter rule name.	string	Maximum length: 35																			
password-protected	Match password-protected files.	option	-	any																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yes</i></td><td>Match only password-protected files.</td></tr><tr><td><i>any</i></td><td>Match any file.</td></tr></table>	Option	Description	<i>yes</i>	Match only password-protected files.	<i>any</i>	Match any file.															
Option	Description																					
<i>yes</i>	Match only password-protected files.																					
<i>any</i>	Match any file.																					
protocol	Protocols to apply rule to.	option	-	http ftp smtp imap pop3 mapi cifs ssh																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>Filter on HTTP.</td></tr><tr><td><i>ftp</i></td><td>Filter on FTP.</td></tr><tr><td><i>smtp</i></td><td>Filter on SMTP.</td></tr><tr><td><i>imap</i></td><td>Filter on IMAP.</td></tr><tr><td><i>pop3</i></td><td>Filter on POP3.</td></tr><tr><td><i>mapi</i></td><td>Filter on MAPI. (Proxy mode only.)</td></tr><tr><td><i>cifs</i></td><td>Filter on CIFS.</td></tr><tr><td><i>ssh</i></td><td>Filter on SFTP and SCP. (Proxy mode only.)</td></tr></table>	Option	Description	<i>http</i>	Filter on HTTP.	<i>ftp</i>	Filter on FTP.	<i>smtp</i>	Filter on SMTP.	<i>imap</i>	Filter on IMAP.	<i>pop3</i>	Filter on POP3.	<i>mapi</i>	Filter on MAPI. (Proxy mode only.)	<i>cifs</i>	Filter on CIFS.	<i>ssh</i>	Filter on SFTP and SCP. (Proxy mode only.)			
Option	Description																					
<i>http</i>	Filter on HTTP.																					
<i>ftp</i>	Filter on FTP.																					
<i>smtp</i>	Filter on SMTP.																					
<i>imap</i>	Filter on IMAP.																					
<i>pop3</i>	Filter on POP3.																					
<i>mapi</i>	Filter on MAPI. (Proxy mode only.)																					
<i>cifs</i>	Filter on CIFS.																					
<i>ssh</i>	Filter on SFTP and SCP. (Proxy mode only.)																					

firewall

This section includes syntax for the following commands:

- [config firewall DoS-policy on page 345](#)
- [config firewall DoS-policy6 on page 348](#)
- [config firewall access-proxy-ssh-client-cert on page 422](#)
- [config firewall access-proxy-virtual-host on page 424](#)
- [config firewall access-proxy on page 350](#)
- [config firewall access-proxy6 on page 386](#)
- [config firewall acl on page 426](#)
- [config firewall acl6 on page 428](#)
- [config firewall address on page 429](#)
- [config firewall address6-template on page 440](#)
- [config firewall address6 on page 435](#)
- [config firewall addrgrp on page 442](#)
- [config firewall addrgrp6 on page 444](#)
- [config firewall auth-portal on page 446](#)
- [config firewall central-snat-map on page 446](#)
- [config firewall city on page 449](#)
- [config firewall country on page 450](#)
- [config firewall decrypted-traffic-mirror on page 451](#)
- [config firewall dnstranslation on page 451](#)
- [config firewall global on page 452](#)
- [config firewall identity-based-route on page 453](#)
- [config firewall interface-policy on page 454](#)
- [config firewall interface-policy6 on page 457](#)
- [config firewall internet-service-addition on page 463](#)
- [config firewall internet-service-append on page 464](#)
- [config firewall internet-service-botnet on page 465](#)
- [config firewall internet-service-custom-group on page 467](#)
- [config firewall internet-service-custom on page 465](#)
- [config firewall internet-service-definition on page 468](#)
- [config firewall internet-service-extension on page 469](#)
- [config firewall internet-service-group on page 473](#)
- [config firewall internet-service-ipbl-reason on page 474](#)
- [config firewall internet-service-ipbl-vendor on page 474](#)
- [config firewall internet-service-list on page 475](#)
- [config firewall internet-service-name on page 475](#)
- [config firewall internet-service-owner on page 476](#)

-
- [config firewall internet-service-reputation on page 477](#)
 - [config firewall internet-service-sld on page 477](#)
 - [config firewall internet-service-subapp on page 478](#)
 - [config firewall internet-service on page 461](#)
 - [config firewall ip-translation on page 489](#)
 - [config firewall ipmacbinding setting on page 479](#)
 - [config firewall ipmacbinding table on page 479](#)
 - [config firewall ippool on page 480](#)
 - [config firewall ippool6 on page 486](#)
 - [config firewall ipv6-eh-filter on page 487](#)
 - [config firewall ldb-monitor on page 490](#)
 - [config firewall local-in-policy on page 492](#)
 - [config firewall local-in-policy6 on page 495](#)
 - [config firewall multicast-address on page 499](#)
 - [config firewall multicast-address6 on page 500](#)
 - [config firewall multicast-policy on page 501](#)
 - [config firewall multicast-policy6 on page 504](#)
 - [config firewall network-service-dynamic on page 506](#)
 - [config firewall on-demand-sniffer on page 507](#)
 - [config firewall policy on page 508](#)
 - [config firewall profile-group on page 534](#)
 - [config firewall profile-protocol-options on page 536](#)
 - [config firewall proxy-address on page 561](#)
 - [config firewall proxy-addgrp on page 566](#)
 - [config firewall proxy-policy on page 567](#)
 - [config firewall region on page 577](#)
 - [config firewall schedule group on page 578](#)
 - [config firewall schedule onetime on page 579](#)
 - [config firewall schedule recurring on page 580](#)
 - [config firewall security-policy on page 581](#)
 - [config firewall service category on page 591](#)
 - [config firewall service custom on page 592](#)
 - [config firewall service group on page 596](#)
 - [config firewall shaper per-ip-shaper on page 597](#)
 - [config firewall shaper traffic-shaper on page 599](#)
 - [config firewall shaping-policy on page 602](#)
 - [config firewall shaping-profile on page 607](#)
 - [config firewall sniffer on page 610](#)
 - [config firewall ssh host-key on page 615](#)
 - [config firewall ssh local-ca on page 617](#)
 - [config firewall ssh local-key on page 618](#)
 - [config firewall ssh setting on page 619](#)
 - [config firewall ssl-server on page 622](#)

- [config firewall ssl-ssh-profile on page 625](#)
- [config firewall ssl setting on page 620](#)
- [config firewall traffic-class on page 656](#)
- [config firewall ttl-policy on page 656](#)
- [config firewall vendor-mac on page 657](#)
- [config firewall vip on page 658](#)
- [config firewall vip6 on page 695](#)
- [config firewall vipgrp on page 729](#)
- [config firewall vipgrp6 on page 729](#)
- [config firewall wildcard-fqdn custom on page 730](#)
- [config firewall wildcard-fqdn group on page 731](#)

config firewall DoS-policy

Configure IPv4 DoS policies.

```
config firewall DoS-policy
  Description: Configure IPv4 DoS policies.
  edit <policyid>
    config anomaly
      Description: Anomaly name.
      edit <name>
        set action [pass|block]
        set log [enable|disable]
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set status [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
      next
    end
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set interface {string}
    set name {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
  next
end
```

config firewall DoS-policy

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 1023							
dstaddr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79							
interface	Incoming interface name from available interfaces.	string	Maximum length: 35							
name	Policy name.	string	Maximum length: 35							
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999 **	0						
service <name>	Service object from available options. Service name.	string	Maximum length: 79							
srcaddr <name>	Source address name from available addresses. Address name.	string	Maximum length: 79							
status	Enable/disable this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this policy.</td></tr><tr><td>disable</td><td>Disable this policy.</td></tr></table>				Option	Description	enable	Enable this policy.	disable	Disable this policy.
Option	Description									
enable	Enable this policy.									
disable	Disable this policy.									

** Values may differ between models.

config anomaly

Parameter	Description	Type	Size	Default						
action	Action taken when the threshold is reached.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Allow traffic but record a log message if logging is enabled.</td></tr><tr><td><i>block</i></td><td>Block traffic if this anomaly is found.</td></tr></table>	Option	Description	<i>pass</i>	Allow traffic but record a log message if logging is enabled.	<i>block</i>	Block traffic if this anomaly is found.			
	Option	Description								
	<i>pass</i>	Allow traffic but record a log message if logging is enabled.								
<i>block</i>	Block traffic if this anomaly is found.									
log	Enable/disable anomaly logging.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
	Option	Description								
	<i>enable</i>	Enable anomaly logging.								
<i>disable</i>	Disable anomaly logging.									
name	Anomaly name.	string	Maximum length: 63							
quarantine	Quarantine method.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Quarantine is disabled.</td></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
	Option	Description								
	<i>none</i>	Quarantine is disabled.								
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. (Format ####d###h###m, minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine logging.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
	Option	Description								
	<i>disable</i>	Disable quarantine logging.								
<i>enable</i>	Enable quarantine logging.									
status	Enable/disable this anomaly.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this status.</td></tr><tr><td><i>enable</i></td><td>Enable this status.</td></tr></table>	Option	Description	<i>disable</i>	Disable this status.	<i>enable</i>	Enable this status.			
	Option	Description								
	<i>disable</i>	Disable this status.								
<i>enable</i>	Enable this status.									
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 0 1 Maximum value: 2147483647							
threshold (default)	Number of detected instances (packets per second or concurrent session number) which triggers action (1 - 2147483647, default = 1000). Note that each anomaly has a different threshold value assigned to it. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							

config firewall DoS-policy6

Configure IPv6 DoS policies.

```
config firewall DoS-policy6
  Description: Configure IPv6 DoS policies.
  edit <policyid>
    config anomaly
      Description: Anomaly name.
      edit <name>
        set action [pass|block]
        set log [enable|disable]
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set status [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
      next
    end
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set interface {string}
    set name {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
  next
end
```

config firewall DoS-policy6

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79	
interface	Incoming interface name from available interfaces.	string	Maximum length: 35	
name	Policy name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999 **	0
service <name>	Service object from available options. Service name.	string	Maximum length: 79	
srcaddr <name>	Source address name from available addresses. Address name.	string	Maximum length: 79	
status	Enable/disable this policy.	option	-	enable
	Option	Description		
	enable	Enable this policy.		
	disable	Disable this policy.		

** Values may differ between models.

config anomaly

Parameter	Description	Type	Size	Default						
action	Action taken when the threshold is reached.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pass</td><td>Allow traffic but record a log message if logging is enabled.</td></tr><tr><td>block</td><td>Block traffic if this anomaly is found.</td></tr></table>	Option	Description	pass	Allow traffic but record a log message if logging is enabled.	block	Block traffic if this anomaly is found.			
Option	Description									
pass	Allow traffic but record a log message if logging is enabled.									
block	Block traffic if this anomaly is found.									
log	Enable/disable anomaly logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable anomaly logging.</td></tr><tr><td>disable</td><td>Disable anomaly logging.</td></tr></table>	Option	Description	enable	Enable anomaly logging.	disable	Disable anomaly logging.			
Option	Description									
enable	Enable anomaly logging.									
disable	Disable anomaly logging.									
name	Anomaly name.	string	Maximum length: 63							
quarantine	Quarantine method.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Quarantine is disabled.</td></tr></table>	Option	Description	none	Quarantine is disabled.					
Option	Description									
none	Quarantine is disabled.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>	Option	Description	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.					
	Option	Description								
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. (Format ####d###h###m, minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine logging.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
	Option	Description								
	<i>disable</i>	Disable quarantine logging.								
<i>enable</i>	Enable quarantine logging.									
status	Enable/disable this anomaly.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this status.</td></tr><tr><td><i>enable</i></td><td>Enable this status.</td></tr></table>	Option	Description	<i>disable</i>	Disable this status.	<i>enable</i>	Enable this status.			
	Option	Description								
	<i>disable</i>	Disable this status.								
<i>enable</i>	Enable this status.									
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 0 1 Maximum value: 2147483647							
threshold (default)	Number of detected instances (packets per second or concurrent session number) which triggers action (1 - 2147483647, default = 1000). Note that each anomaly has a different threshold value assigned to it. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							

config firewall access-proxy

Configure IPv4 access proxy.

```
config firewall access-proxy
  Description: Configure IPv4 access proxy.
  edit <name>
    set add-vhost-domain-to-dnsdb [enable|disable]
  config api-gateway
    Description: Set IPv4 API Gateway.
    edit <id>
      set application <name1>, <name2>, ...
```

```

set h2-support [enable|disable]
set h3-support [enable|disable]
set http-cookie-age {integer}
set http-cookie-domain {string}
set http-cookie-domain-from-host [disable|enable]
set http-cookie-generation {integer}
set http-cookie-path {string}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set ldb-method [static|round-robin|...]
set persistence [none|http-cookie]
config quic
    Description: QUIC setting.
    set ack-delay-exponent {integer}
    set active-connection-id-limit {integer}
    set active-migration [enable|disable]
    set grease-quic-bit [enable|disable]
    set max-ack-delay {integer}
    set max-datagram-frame-size {integer}
    set max-idle-timeout {integer}
    set max-udp-payload-size {integer}
end
config realservers
    Description: Select the real servers that this Access Proxy will distribute
traffic to.
    edit <id>
        set addr-type [ip|fqdn]
        set address {string}
        set domain {string}
        set external-auth [enable|disable]
        set health-check [disable|enable]
        set health-check-proto [ping|http|...]
        set holddown-interval [enable|disable]
        set http-host {string}
        set ip {ipv4-address-any}
        set mappedport {user}
        set port {integer}
        set ssh-client-cert {string}
        set ssh-host-key <name1>, <name2>, ...
        set ssh-host-key-validation [disable|enable]
        set status [active|standby|...]
        set translate-host [enable|disable]
        set tunnel-encryption [enable|disable]
        set type [tcp-forwarding|ssh]
        set verify-cert [enable|disable]
        set weight {integer}
    next
end
set saml-redirect [disable|enable]
set saml-server {string}
set service [http|https|...]
set ssl-algorithm [high|medium|...]

```

```

config ssl-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-dh-bits [768|1024|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-min-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
set ssl-vpn-web-portal {string}
set url-map {string}
set url-map-type [sub-string|wildcard|...]
set virtual-host {string}
next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set application <name1>, <name2>, ...
        set h2-support [enable|disable]
        set h3-support [enable|disable]
        set http-cookie-age {integer}
        set http-cookie-domain {string}
        set http-cookie-domain-from-host [disable|enable]
        set http-cookie-generation {integer}
        set http-cookie-path {string}
        set http-cookie-share [disable|same-ip]
        set https-cookie-secure [disable|enable]
        set ldb-method [static|round-robin|...]
        set persistence [none|http-cookie]
    config quic
        Description: QUIC setting.
        set ack-delay-exponent {integer}
        set active-connection-id-limit {integer}
        set active-migration [enable|disable]
        set grease-quic-bit [enable|disable]
        set max-ack-delay {integer}
        set max-datagram-frame-size {integer}
        set max-idle-timeout {integer}
        set max-udp-payload-size {integer}
    end
    config realservers
        Description: Select the real servers that this Access Proxy will distribute
traffic to.
        edit <id>
            set addr-type [ip|fqdn]
            set address {string}
            set domain {string}
            set external-auth [enable|disable]
            set health-check [disable|enable]

```



```

        set health-check-proto [ping|http|...]
        set holddown-interval [enable|disable]
        set http-host {string}
        set ip {ipv6-address}
        set mappedport {user}
        set port {integer}
        set ssh-client-cert {string}
        set ssh-host-key <name1>, <name2>, ...
        set ssh-host-key-validation [disable|enable]
        set status [active|standby|...]
        set translate-host [enable|disable]
        set tunnel-encryption [enable|disable]
        set type [tcp-forwarding|ssh]
        set verify-cert [enable|disable]
        set weight {integer}
    next
end
set saml-redirect [disable|enable]
set saml-server {string}
set service [http|https|...]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-dh-bits [768|1024|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-min-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
set ssl-vpn-web-portal {string}
set url-map {string}
set url-map-type [sub-string|wildcard|...]
set virtual-host {string}
next
end
set auth-portal [disable|enable]
set auth-virtual-host {string}
set decrypted-traffic-mirror {string}
set log-blocked-traffic [enable|disable]
set svr-pool-multiplex [enable|disable]
set svr-pool-server-max-concurrent-request {integer}
set svr-pool-server-max-request {integer}
set svr-pool-ttl {integer}
set vip {string}
next
end

```

config firewall access-proxy

Parameter	Description	Type	Size	Default						
add-vhost-domain-to-dnsdb	Enable/disable adding vhost/domain to dnsdb for ztna dox tunnel.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>add dns entry for all vhosts used by access proxy.</td></tr><tr><td>disable</td><td>Do not add dns entry for all vhosts used by access proxy.</td></tr></table>	Option	Description	enable	add dns entry for all vhosts used by access proxy.	disable	Do not add dns entry for all vhosts used by access proxy.			
Option	Description									
enable	add dns entry for all vhosts used by access proxy.									
disable	Do not add dns entry for all vhosts used by access proxy.									
auth-portal	Enable/disable authentication portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable authentication portal.</td></tr><tr><td>enable</td><td>Enable authentication portal.</td></tr></table>	Option	Description	disable	Disable authentication portal.	enable	Enable authentication portal.			
Option	Description									
disable	Disable authentication portal.									
enable	Enable authentication portal.									
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79							
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Log all traffic denied by this access proxy.</td></tr><tr><td>disable</td><td>Do not log all traffic denied by this access proxy.</td></tr></table>	Option	Description	enable	Log all traffic denied by this access proxy.	disable	Do not log all traffic denied by this access proxy.			
Option	Description									
enable	Log all traffic denied by this access proxy.									
disable	Do not log all traffic denied by this access proxy.									
name	Access Proxy name.	string	Maximum length: 79							
svr-pool-multiplex	Enable/disable server pool multiplexing. Share connected server in HTTP, HTTPS, and web-portal api-gateway.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable server pool multiplexing. Share connected server.</td></tr><tr><td>disable</td><td>Disable server pool multiplexing. Do not share connected server.</td></tr></table>	Option	Description	enable	Enable server pool multiplexing. Share connected server.	disable	Disable server pool multiplexing. Do not share connected server.			
Option	Description									
enable	Enable server pool multiplexing. Share connected server.									
disable	Disable server pool multiplexing. Do not share connected server.									

Parameter	Description	Type	Size	Default
svr-pool-server-max-concurrent-request	Maximum number of concurrent requests that servers in server pool could handle (default = unlimited).	integer	Minimum value: 0 Maximum value: 2147483647	0
svr-pool-server-max-request	Maximum number of requests that servers in server pool handle before disconnecting (default = unlimited).	integer	Minimum value: 0 Maximum value: 2147483647	0
svr-pool-ttl	Time-to-live in the server pool for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15
vip	Virtual IP name.	string	Maximum length: 79	

config api-gateway

Parameter	Description	Type	Size	Default						
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79							
h2-support	HTTP2 support, default=Enable.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP2 support.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP2 support.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP2 support.	<i>disable</i>	Disable HTTP2 support.			
Option	Description									
<i>enable</i>	Enable HTTP2 support.									
<i>disable</i>	Disable HTTP2 support.									
h3-support	HTTP3/QUIC support, default=Disable.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP3/QUIC support.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP3/QUIC support.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP3/QUIC support.	<i>disable</i>	Disable HTTP3/QUIC support.			
Option	Description									
<i>enable</i>	Enable HTTP3/QUIC support.									
<i>disable</i>	Disable HTTP3/QUIC support.									
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td>enable</td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>				Option	Description	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).	enable	Enable use of HTTP cookie domain from host field in HTTP.
	Option	Description								
	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).								
enable	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 0 Maximum value: 4294967295							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Only allow HTTP cookie to match this API Gateway.</td></tr><tr><td>same-ip</td><td>Allow HTTP cookie to match any API Gateway with same IP.</td></tr></table>				Option	Description	disable	Only allow HTTP cookie to match this API Gateway.	same-ip	Allow HTTP cookie to match any API Gateway with same IP.
	Option	Description								
	disable	Only allow HTTP cookie to match this API Gateway.								
same-ip	Allow HTTP cookie to match any API Gateway with same IP.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td>enable</td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>				Option	Description	disable	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	enable	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.
	Option	Description								
	disable	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.								
enable	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.									
id	API Gateway ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
ldb-method	Method used to distribute sessions to real servers.	option	-	static						

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute to server based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute to server based round robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute to server based on weight.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	<i>static</i>	Distribute to server based on source IP.	<i>round-robin</i>	Distribute to server based round robin order.	<i>weighted</i>	Distribute to server based on weight.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.					
	Option	Description																
	<i>static</i>	Distribute to server based on source IP.																
	<i>round-robin</i>	Distribute to server based round robin order.																
	<i>weighted</i>	Distribute to server based on weight.																
	<i>first-alive</i>	Distribute to the first server that is alive.																
<i>http-host</i>	Distribute to server based on host field in HTTP header.																	
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.											
	Option	Description																
	<i>none</i>	None.																
<i>http-cookie</i>	HTTP cookie.																	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not support redirection after successful SAML authentication.</td></tr><tr><td><i>enable</i></td><td>Support redirection after successful SAML authentication.</td></tr></table>	Option	Description	<i>disable</i>	Do not support redirection after successful SAML authentication.	<i>enable</i>	Support redirection after successful SAML authentication.											
	Option	Description																
	<i>disable</i>	Do not support redirection after successful SAML authentication.																
<i>enable</i>	Support redirection after successful SAML authentication.																	
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35															
service	Service.	option	-	https														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>tcp-forwarding</i></td><td>TCP-FORWARDING.</td></tr><tr><td><i>samlsp</i></td><td>SAML-SP.</td></tr><tr><td><i>web-portal</i></td><td>VPN-SSL-WEB-PORTAL.</td></tr><tr><td><i>saas</i></td><td>SAAS.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.	<i>tcp-forwarding</i>	TCP-FORWARDING.	<i>samlsp</i>	SAML-SP.	<i>web-portal</i>	VPN-SSL-WEB-PORTAL.	<i>saas</i>	SAAS.			
	Option	Description																
	<i>http</i>	HTTP.																
	<i>https</i>	HTTPS.																
	<i>tcp-forwarding</i>	TCP-FORWARDING.																
	<i>samlsp</i>	SAML-SP.																
	<i>web-portal</i>	VPN-SSL-WEB-PORTAL.																
<i>saas</i>	SAAS.																	
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high														

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.									
	Option	Description																
	<i>high</i>	High encryption. Allow only AES and ChaCha.																
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.			
	Option	Description																
	768	768-bit Diffie-Hellman prime.																
	1024	1024-bit Diffie-Hellman prime.																
	1536	1536-bit Diffie-Hellman prime.																
	2048	2048-bit Diffie-Hellman prime.																
	3072	3072-bit Diffie-Hellman prime.																
4096	4096-bit Diffie-Hellman prime.																	
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																	
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																	
ssl-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable secure renegotiation.		
	<i>disable</i>	Disable secure renegotiation.		
ssl-vpn-web-portal *	Agentless VPN web portal.	string	Maximum length: 35	
url-map	URL pattern to match.	string	Maximum length: 511	/
url-map-type	Type of url-map.	option	-	sub-string
	Option	Description		
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.		
	<i>wildcard</i>	Match the pattern with wildcards.		
	<i>regex</i>	Match the pattern with a regular expression.		
virtual-host	Virtual host.	string	Maximum length: 79	

* This parameter may not exist in some models.

config quic

Parameter	Description	Type	Size	Default						
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3						
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2						
active-migration	Enable/disable active migration (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable active migration.</td></tr><tr><td><i>disable</i></td><td>Disable active migration.</td></tr></table>				Option	Description	<i>enable</i>	Enable active migration.	<i>disable</i>	Disable active migration.
Option	Description									
<i>enable</i>	Enable active migration.									
<i>disable</i>	Disable active migration.									
grease-quic-bit	Enable/disable grease QUIC bit (default = enable).	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable grease QUIC bit.		
	<i>disable</i>	Disable grease QUIC bit.		
max-ack-delay	Maximum ACK delay in milliseconds (1 - 16383, default = 25).	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes (1 - 1500, default = 1500).	integer	Minimum value: 1 Maximum value: 1500	1500
max-idle-timeout	Maximum idle timeout milliseconds (1 - 60000, default = 30000).	integer	Minimum value: 1 Maximum value: 60000	30000
max-udp-payload-size	Maximum UDP payload size in bytes (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500

config realservers

Parameter	Description	Type	Size	Default						
addr-type	Type of address.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Non-wildcard FQDN address object.</td></tr></table>				Option	Description	<i>ip</i>	Standard IPv4 address.	<i>fqdn</i>	Non-wildcard FQDN address object.
	Option	Description								
	<i>ip</i>	Standard IPv4 address.								
<i>fqdn</i>	Non-wildcard FQDN address object.									
address	Address or address group of the real server.	string	Maximum length: 79							
domain	Wildcard domain name of the real server.	string	Maximum length: 255							
external-auth	Enable/disable use of external browser as user-agent for SAML user authentication.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of external browser as user-agent for SAML user authentication.</td></tr><tr><td><i>disable</i></td><td>Disable use of external browser as user-agent for SAML user authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of external browser as user-agent for SAML user authentication.	<i>disable</i>	Disable use of external browser as user-agent for SAML user authentication.					
	Option	Description										
	<i>enable</i>	Enable use of external browser as user-agent for SAML user authentication.										
<i>disable</i>	Disable use of external browser as user-agent for SAML user authentication.											
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr></table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.					
	Option	Description										
	<i>disable</i>	Disable per server health check.										
<i>enable</i>	Enable per server health check.											
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>Use PING to test the link with the server.</td></tr><tr><td><i>http</i></td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td><i>tcp-connect</i></td><td>Use a full TCP connection to test the link with the server.</td></tr></table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.			
	Option	Description										
	<i>ping</i>	Use PING to test the link with the server.										
	<i>http</i>	Use HTTP-GET to test the link with the server.										
<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.											
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per server holddown.</td></tr><tr><td><i>disable</i></td><td>Disable per server holddown.</td></tr></table>	Option	Description	<i>enable</i>	Enable per server holddown.	<i>disable</i>	Disable per server holddown.					
	Option	Description										
	<i>enable</i>	Enable per server holddown.										
<i>disable</i>	Disable per server holddown.											
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295									
ip	IP address of the real server.	ipv4-address-any	Not Specified	0.0.0.0								
mappedport	Port for communicating with the real server.	user	Not Specified									

Parameter	Description	Type	Size	Default								
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79									
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79									
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SSH real server host key validation.</td></tr><tr><td>enable</td><td>Enable SSH real server host key validation.</td></tr></table>				Option	Description	disable	Disable SSH real server host key validation.	enable	Enable SSH real server host key validation.		
Option	Description											
disable	Disable SSH real server host key validation.											
enable	Enable SSH real server host key validation.											
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>active</td><td>Server status active.</td></tr><tr><td>standby</td><td>Server status standby.</td></tr><tr><td>disable</td><td>Server status disable.</td></tr></table>				Option	Description	active	Server status active.	standby	Server status standby.	disable	Server status disable.
Option	Description											
active	Server status active.											
standby	Server status standby.											
disable	Server status disable.											
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable virtual hostname/IP translation.</td></tr><tr><td>disable</td><td>Disable virtual hostname/IP translation.</td></tr></table>				Option	Description	enable	Enable virtual hostname/IP translation.	disable	Disable virtual hostname/IP translation.		
Option	Description											
enable	Enable virtual hostname/IP translation.											
disable	Disable virtual hostname/IP translation.											
tunnel-encryption	Tunnel encryption.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable tcp forwarding tunnel encryption.</td></tr><tr><td>disable</td><td>Disable tcp forwarding tunnel encryption.</td></tr></table>				Option	Description	enable	Enable tcp forwarding tunnel encryption.	disable	Disable tcp forwarding tunnel encryption.		
Option	Description											
enable	Enable tcp forwarding tunnel encryption.											
disable	Disable tcp forwarding tunnel encryption.											
type	TCP forwarding server type.	option	-	tcp-forwarding								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tcp-forwarding</i>	TCP forwarding.		
	<i>ssh</i>	SSH.		
verify-cert	Enable/disable certificate verification of the real server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable certificate verification.		
	<i>disable</i>	Disable certificate verification.		
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default												
cipher	Cipher suite name.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-AES-128-GCM-SHA256</td><td>Cipher suite TLS-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-AES-256-GCM-SHA384</td><td>Cipher suite TLS-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr></table>				Option	Description	TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.	TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.	TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
Option	Description															
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.															
TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.															
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.															
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.															
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																				
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																				
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																				
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																				
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																				
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																					
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295																			
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.											
	Option	Description																				
	<i>tls-1.0</i>	TLS 1.0.																				
	<i>tls-1.1</i>	TLS 1.1.																				
	<i>tls-1.2</i>	TLS 1.2.																				
<i>tls-1.3</i>	TLS 1.3.																					

config api-gateway6

Parameter	Description	Type	Size	Default						
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79							
h2-support	HTTP2 support, default=Enable.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP2 support.</td></tr><tr><td>disable</td><td>Disable HTTP2 support.</td></tr></table>	Option	Description	enable	Enable HTTP2 support.	disable	Disable HTTP2 support.			
	Option	Description								
	enable	Enable HTTP2 support.								
disable	Disable HTTP2 support.									
h3-support	HTTP3/QUIC support, default=Disable.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP3/QUIC support.</td></tr><tr><td>disable</td><td>Disable HTTP3/QUIC support.</td></tr></table>	Option	Description	enable	Enable HTTP3/QUIC support.	disable	Disable HTTP3/QUIC support.			
	Option	Description								
	enable	Enable HTTP3/QUIC support.								
disable	Disable HTTP3/QUIC support.									
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td>enable</td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>	Option	Description	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).	enable	Enable use of HTTP cookie domain from host field in HTTP.			
	Option	Description								
	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).								
enable	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Only allow HTTP cookie to match this API Gateway.</td></tr><tr><td><i>same-ip</i></td><td>Allow HTTP cookie to match any API Gateway with same IP.</td></tr></table>	Option	Description	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.									
	Option	Description														
	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.														
<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.															
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td><i>enable</i></td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>	Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.									
	Option	Description														
	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.														
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.															
id	API Gateway ID.	integer	Minimum value: 0 0 Maximum value: 4294967295													
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute to server based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute to server based round robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute to server based on weight.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	<i>static</i>	Distribute to server based on source IP.	<i>round-robin</i>	Distribute to server based round robin order.	<i>weighted</i>	Distribute to server based on weight.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.			
	Option	Description														
	<i>static</i>	Distribute to server based on source IP.														
	<i>round-robin</i>	Distribute to server based round robin order.														
	<i>weighted</i>	Distribute to server based on weight.														
	<i>first-alive</i>	Distribute to the first server that is alive.														
<i>http-host</i>	Distribute to server based on host field in HTTP header.															
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.									
	Option	Description														
	<i>none</i>	None.														
<i>http-cookie</i>	HTTP cookie.															
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	enable												

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not support redirection after successful SAML authentication.</td></tr><tr><td><i>enable</i></td><td>Support redirection after successful SAML authentication.</td></tr></table>	Option	Description	<i>disable</i>	Do not support redirection after successful SAML authentication.	<i>enable</i>	Support redirection after successful SAML authentication.											
	Option	Description																
	<i>disable</i>	Do not support redirection after successful SAML authentication.																
<i>enable</i>	Support redirection after successful SAML authentication.																	
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35															
service	Service.	option	-	https														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>tcp-forwarding</i></td><td>TCP-FORWARDING.</td></tr><tr><td><i>samlsp</i></td><td>SAML-SP.</td></tr><tr><td><i>web-portal</i></td><td>VPN-SSL-WEB-PORTAL.</td></tr><tr><td><i>saas</i></td><td>SAAS.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.	<i>tcp-forwarding</i>	TCP-FORWARDING.	<i>samlsp</i>	SAML-SP.	<i>web-portal</i>	VPN-SSL-WEB-PORTAL.	<i>saas</i>	SAAS.			
	Option	Description																
	<i>http</i>	HTTP.																
	<i>https</i>	HTTPS.																
	<i>tcp-forwarding</i>	TCP-FORWARDING.																
	<i>samlsp</i>	SAML-SP.																
	<i>web-portal</i>	VPN-SSL-WEB-PORTAL.																
<i>saas</i>	SAAS.																	
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.									
	Option	Description																
	<i>high</i>	High encryption. Allow only AES and ChaCha.																
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td><i>3072</i></td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td><i>4096</i></td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.			
	Option	Description																
	<i>768</i>	768-bit Diffie-Hellman prime.																
	<i>1024</i>	1024-bit Diffie-Hellman prime.																
	<i>1536</i>	1536-bit Diffie-Hellman prime.																
	<i>2048</i>	2048-bit Diffie-Hellman prime.																
<i>3072</i>	3072-bit Diffie-Hellman prime.																	
<i>4096</i>	4096-bit Diffie-Hellman prime.																	

Parameter	Description	Type	Size	Default										
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.			
	Option	Description												
	tls-1.0	TLS 1.0.												
	tls-1.1	TLS 1.1.												
	tls-1.2	TLS 1.2.												
tls-1.3	TLS 1.3.													
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.			
	Option	Description												
	tls-1.0	TLS 1.0.												
	tls-1.1	TLS 1.1.												
	tls-1.2	TLS 1.2.												
tls-1.3	TLS 1.3.													
ssl-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable secure renegotiation.</td></tr><tr><td>disable</td><td>Disable secure renegotiation.</td></tr></table>	Option	Description	enable	Enable secure renegotiation.	disable	Disable secure renegotiation.							
	Option	Description												
	enable	Enable secure renegotiation.												
disable	Disable secure renegotiation.													
ssl-vpn-web-portal *	Agentless VPN web portal.	string	Maximum length: 35											
url-map	URL pattern to match.	string	Maximum length: 511	/										
url-map-type	Type of url-map.	option	-	sub-string										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sub-string</td><td>Match the pattern if a string contains the sub-string.</td></tr><tr><td>wildcard</td><td>Match the pattern with wildcards.</td></tr><tr><td>regex</td><td>Match the pattern with a regular expression.</td></tr></table>	Option	Description	sub-string	Match the pattern if a string contains the sub-string.	wildcard	Match the pattern with wildcards.	regex	Match the pattern with a regular expression.					
	Option	Description												
	sub-string	Match the pattern if a string contains the sub-string.												
	wildcard	Match the pattern with wildcards.												
regex	Match the pattern with a regular expression.													
virtual-host	Virtual host.	string	Maximum length: 79											

* This parameter may not exist in some models.

config quic

Parameter	Description	Type	Size	Default
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2
active-migration	Enable/disable active migration (default = disable).	option	-	disable
	Option Description			
	enable Enable active migration.			
	disable Disable active migration.			
grease-quic-bit	Enable/disable grease QUIC bit (default = enable).	option	-	enable
	Option Description			
	enable Enable grease QUIC bit.			
	disable Disable grease QUIC bit.			
max-ack-delay	Maximum ACK delay in milliseconds (1 - 16383, default = 25).	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes (1 - 1500, default = 1500).	integer	Minimum value: 1 Maximum value: 1500	1500
max-idle-timeout	Maximum idle timeout milliseconds (1 - 60000, default = 30000).	integer	Minimum value: 1 Maximum value: 60000	30000
max-udp-payload-size	Maximum UDP payload size in bytes (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500

config realservers

Parameter	Description	Type	Size	Default								
addr-type	Type of address.	option	-	ip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ip</td><td>Standard IPv4 address.</td></tr><tr><td>fqdn</td><td>Non-wildcard FQDN address object.</td></tr></table>	Option	Description	ip	Standard IPv4 address.	fqdn	Non-wildcard FQDN address object.					
Option	Description											
ip	Standard IPv4 address.											
fqdn	Non-wildcard FQDN address object.											
address	Address or address group of the real server.	string	Maximum length: 79									
domain	Wildcard domain name of the real server.	string	Maximum length: 255									
external-auth	Enable/disable use of external browser as user-agent for SAML user authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of external browser as user-agent for SAML user authentication.</td></tr><tr><td>disable</td><td>Disable use of external browser as user-agent for SAML user authentication.</td></tr></table>	Option	Description	enable	Enable use of external browser as user-agent for SAML user authentication.	disable	Disable use of external browser as user-agent for SAML user authentication.					
Option	Description											
enable	Enable use of external browser as user-agent for SAML user authentication.											
disable	Disable use of external browser as user-agent for SAML user authentication.											
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable per server health check.</td></tr><tr><td>enable</td><td>Enable per server health check.</td></tr></table>	Option	Description	disable	Disable per server health check.	enable	Enable per server health check.					
Option	Description											
disable	Disable per server health check.											
enable	Enable per server health check.											
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>Use PING to test the link with the server.</td></tr><tr><td>http</td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td>tcp-connect</td><td>Use a full TCP connection to test the link with the server.</td></tr></table>	Option	Description	ping	Use PING to test the link with the server.	http	Use HTTP-GET to test the link with the server.	tcp-connect	Use a full TCP connection to test the link with the server.			
Option	Description											
ping	Use PING to test the link with the server.											
http	Use HTTP-GET to test the link with the server.											
tcp-connect	Use a full TCP connection to test the link with the server.											
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable per server holddown.		
	<i>disable</i>	Disable per server holddown.		
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::
mappedport	Port for communicating with the real server.	user	Not Specified	
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79	
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable
	Option Description			
	<i>disable</i>	Disable SSH real server host key validation.		
	<i>enable</i>	Enable SSH real server host key validation.		
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active
	Option Description			
	<i>active</i>	Server status active.		
	<i>standby</i>	Server status standby.		
	<i>disable</i>	Server status disable.		
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable virtual hostname/IP translation.		
	<i>disable</i>	Disable virtual hostname/IP translation.		
tunnel-encryption	Tunnel encryption.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp forwarding tunnel encryption.		
	<i>disable</i>	Disable tcp forwarding tunnel encryption.		
type	TCP forwarding server type.	option	-	tcp-forwarding
	Option	Description		
	<i>tcp-forwarding</i>	TCP forwarding.		
	<i>ssh</i>	SSH.		
verify-cert	Enable/disable certificate verification of the real server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable certificate verification.		
	<i>disable</i>	Disable certificate verification.		
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	
	Option	Description		
	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.		
	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr></table>	Option	Description	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.			
Option	Description																									
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.																									
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																									
<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.																									
<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																									
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																									
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																									

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.			
Option	Description																									
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.																									
<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.																									
<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.																									
<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.																									
<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.																									
<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.																									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.			
Option	Description																									
<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																									
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.																									

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																								
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																								
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																								
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																								
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																								
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																								
<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																									
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																									
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295																							

Parameter	Description	Type	Size	Default
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3

Option	Description
<i>tls-1.0</i>	TLS 1.0.
<i>tls-1.1</i>	TLS 1.1.
<i>tls-1.2</i>	TLS 1.2.
<i>tls-1.3</i>	TLS 1.3.

config firewall access-proxy6

Configure IPv6 access proxy.

```
config firewall access-proxy6
    Description: Configure IPv6 access proxy.
    edit <name>
        set add-vhost-domain-to-dnsdb [enable|disable]
        config api-gateway
            Description: Set IPv4 API Gateway.
            edit <id>
                set application <name1>, <name2>, ...
                set h2-support [enable|disable]
                set h3-support [enable|disable]
                set http-cookie-age {integer}
                set http-cookie-domain {string}
                set http-cookie-domain-from-host [disable|enable]
                set http-cookie-generation {integer}
                set http-cookie-path {string}
                set http-cookie-share [disable|same-ip]
                set https-cookie-secure [disable|enable]
                set ldb-method [static|round-robin|...]
                set persistence [none|http-cookie]
            config quic
                Description: QUIC setting.
                set ack-delay-exponent {integer}
                set active-connection-id-limit {integer}
                set active-migration [enable|disable]
                set grease-quic-bit [enable|disable]
                set max-ack-delay {integer}
                set max-datagram-frame-size {integer}
                set max-idle-timeout {integer}
                set max-udp-payload-size {integer}
            end
        config realservers
```

```

Description: Select the real servers that this Access Proxy will distribute
traffic to.
edit <id>
    set addr-type [ip|fqdn]
    set address {string}
    set domain {string}
    set external-auth [enable|disable]
    set health-check [disable|enable]
    set health-check-proto [ping|http|...]
    set holddown-interval [enable|disable]
    set http-host {string}
    set ip {ipv4-address-any}
    set mappedport {user}
    set port {integer}
    set ssh-client-cert {string}
    set ssh-host-key <name1>, <name2>, ...
    set ssh-host-key-validation [disable|enable]
    set status [active|standby|...]
    set translate-host [enable|disable]
    set tunnel-encryption [enable|disable]
    set type [tcp-forwarding|ssh]
    set verify-cert [enable|disable]
    set weight {integer}
next
end
set saml-redirect [disable|enable]
set saml-server {string}
set service [http|https|...]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-dh-bits [768|1024|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-min-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
set ssl-vpn-web-portal {string}
set url-map {string}
set url-map-type [sub-string|wildcard|...]
set virtual-host {string}
next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set application <name1>, <name2>, ...
        set h2-support [enable|disable]
        set h3-support [enable|disable]

```

```

set http-cookie-age {integer}
set http-cookie-domain {string}
set http-cookie-domain-from-host [disable|enable]
set http-cookie-generation {integer}
set http-cookie-path {string}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set ldb-method [static|round-robin|...]
set persistence [none|http-cookie]
config quic
    Description: QUIC setting.
    set ack-delay-exponent {integer}
    set active-connection-id-limit {integer}
    set active-migration [enable|disable]
    set grease-quic-bit [enable|disable]
    set max-ack-delay {integer}
    set max-datagram-frame-size {integer}
    set max-idle-timeout {integer}
    set max-udp-payload-size {integer}
end
config realservers
    Description: Select the real servers that this Access Proxy will distribute
traffic to.
    edit <id>
        set addr-type [ip|fqdn]
        set address {string}
        set domain {string}
        set external-auth [enable|disable]
        set health-check [disable|enable]
        set health-check-proto [ping|http|...]
        set holddown-interval [enable|disable]
        set http-host {string}
        set ip {ipv6-address}
        set mappedport {user}
        set port {integer}
        set ssh-client-cert {string}
        set ssh-host-key <name1>, <name2>, ...
        set ssh-host-key-validation [disable|enable]
        set status [active|standby|...]
        set translate-host [enable|disable]
        set tunnel-encryption [enable|disable]
        set type [tcp-forwarding|ssh]
        set verify-cert [enable|disable]
        set weight {integer}
    next
end
set saml-redirect [disable|enable]
set saml-server {string}
set service [http|https|...]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.

```

```

        edit <priority>
            set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
            set versions {option1}, {option2}, ...
        next
    end
    set ssl-dh-bits [768|1024|...]
    set ssl-max-version [tls-1.0|tls-1.1|...]
    set ssl-min-version [tls-1.0|tls-1.1|...]
    set ssl-renegotiation [enable|disable]
    set ssl-vpn-web-portal {string}
    set url-map {string}
    set url-map-type [sub-string|wildcard|...]
    set virtual-host {string}
next
end
set auth-portal [disable|enable]
set auth-virtual-host {string}
set decrypted-traffic-mirror {string}
set log-blocked-traffic [enable|disable]
set svr-pool-multiplex [enable|disable]
set svr-pool-server-max-concurrent-request {integer}
set svr-pool-server-max-request {integer}
set svr-pool-ttl {integer}
set vip {string}
next
end

```

config firewall access-proxy6

Parameter	Description	Type	Size	Default
add-vhost-domain-to-dnsdb	Enable/disable adding vhost/domain to dnsdb for ztna dox tunnel.	option	-	disable
	Option	Description		
	<i>enable</i>	add dns entry for all vhosts used by access proxy.		
	<i>disable</i>	Do not add dns entry for all vhosts used by access proxy.		
auth-portal	Enable/disable authentication portal.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable authentication portal.		
	<i>enable</i>	Enable authentication portal.		
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35	
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	enable
	Option	Description		
	enable	Log all traffic denied by this access proxy.		
	disable	Do not log all traffic denied by this access proxy.		
name	Access Proxy name.	string	Maximum length: 79	
svr-pool-multiplex	Enable/disable server pool multiplexing. Share connected server in HTTP, HTTPS, and web-portal api-gateway.	option	-	enable
	Option	Description		
	enable	Enable server pool multiplexing. Share connected server.		
	disable	Disable server pool multiplexing. Do not share connected server.		
svr-pool-server-max-concurrent-request	Maximum number of concurrent requests that servers in server pool could handle (default = unlimited).	integer	Minimum value: 0 Maximum value: 2147483647	0
svr-pool-server-max-request	Maximum number of requests that servers in server pool handle before disconnecting (default = unlimited).	integer	Minimum value: 0 Maximum value: 2147483647	0
svr-pool-ttl	Time-to-live in the server pool for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15
vip	Virtual IP name.	string	Maximum length: 79	

config api-gateway

Parameter	Description	Type	Size	Default
application <name>	SaaS application controlled by this Access Proxy.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
	SaaS application name.									
h2-support	HTTP2 support, default=Enable.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP2 support.</td></tr><tr><td>disable</td><td>Disable HTTP2 support.</td></tr></table>	Option	Description	enable	Enable HTTP2 support.	disable	Disable HTTP2 support.			
Option	Description									
enable	Enable HTTP2 support.									
disable	Disable HTTP2 support.									
h3-support	HTTP3/QUIC support, default=Disable.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP3/QUIC support.</td></tr><tr><td>disable</td><td>Disable HTTP3/QUIC support.</td></tr></table>	Option	Description	enable	Enable HTTP3/QUIC support.	disable	Disable HTTP3/QUIC support.			
Option	Description									
enable	Enable HTTP3/QUIC support.									
disable	Disable HTTP3/QUIC support.									
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td>enable</td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>	Option	Description	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).	enable	Enable use of HTTP cookie domain from host field in HTTP.			
Option	Description									
disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).									
enable	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Only allow HTTP cookie to match this API Gateway.</td></tr></table>	Option	Description	disable	Only allow HTTP cookie to match this API Gateway.					
Option	Description									
disable	Only allow HTTP cookie to match this API Gateway.									

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>same-ip</i></td><td>Allow HTTP cookie to match any API Gateway with same IP.</td></tr></table>		Option	Description	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.										
	Option	Description														
	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.														
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td><i>enable</i></td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>		Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.								
	Option	Description														
	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.														
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.															
id	API Gateway ID.	integer	Minimum value: 0 0 Maximum value: 4294967295													
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute to server based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute to server based round robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute to server based on weight.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to server based on host field in HTTP header.</td></tr></table>		Option	Description	<i>static</i>	Distribute to server based on source IP.	<i>round-robin</i>	Distribute to server based round robin order.	<i>weighted</i>	Distribute to server based on weight.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.		
	Option	Description														
	<i>static</i>	Distribute to server based on source IP.														
	<i>round-robin</i>	Distribute to server based round robin order.														
	<i>weighted</i>	Distribute to server based on weight.														
	<i>first-alive</i>	Distribute to the first server that is alive.														
<i>http-host</i>	Distribute to server based on host field in HTTP header.															
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr></table>		Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.								
	Option	Description														
	<i>none</i>	None.														
<i>http-cookie</i>	HTTP cookie.															
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not support redirection after successful SAML authentication.</td></tr></table>		Option	Description	<i>disable</i>	Do not support redirection after successful SAML authentication.										
	Option	Description														
<i>disable</i>	Do not support redirection after successful SAML authentication.															

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Support redirection after successful SAML authentication.</td></tr></table>	Option	Description	<i>enable</i>	Support redirection after successful SAML authentication.													
	Option	Description																
<i>enable</i>	Support redirection after successful SAML authentication.																	
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35															
service	Service.	option	-	https														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>tcp-forwarding</i></td><td>TCP-FORWARDING.</td></tr><tr><td><i>samlsp</i></td><td>SAML-SP.</td></tr><tr><td><i>web-portal</i></td><td>VPN-SSL-WEB-PORTAL.</td></tr><tr><td><i>saas</i></td><td>SAAS.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.	<i>tcp-forwarding</i>	TCP-FORWARDING.	<i>samlsp</i>	SAML-SP.	<i>web-portal</i>	VPN-SSL-WEB-PORTAL.	<i>saas</i>	SAAS.			
	Option	Description																
	<i>http</i>	HTTP.																
	<i>https</i>	HTTPS.																
	<i>tcp-forwarding</i>	TCP-FORWARDING.																
	<i>samlsp</i>	SAML-SP.																
	<i>web-portal</i>	VPN-SSL-WEB-PORTAL.																
<i>saas</i>	SAAS.																	
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.									
	Option	Description																
	<i>high</i>	High encryption. Allow only AES and ChaCha.																
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td><i>3072</i></td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td><i>4096</i></td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.			
	Option	Description																
	<i>768</i>	768-bit Diffie-Hellman prime.																
	<i>1024</i>	1024-bit Diffie-Hellman prime.																
	<i>1536</i>	1536-bit Diffie-Hellman prime.																
	<i>2048</i>	2048-bit Diffie-Hellman prime.																
	<i>3072</i>	3072-bit Diffie-Hellman prime.																
<i>4096</i>	4096-bit Diffie-Hellman prime.																	
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3														

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description												
	<i>tls-1.0</i>	TLS 1.0.												
	<i>tls-1.1</i>	TLS 1.1.												
	<i>tls-1.2</i>	TLS 1.2.												
<i>tls-1.3</i>	TLS 1.3.													
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description												
	<i>tls-1.0</i>	TLS 1.0.												
	<i>tls-1.1</i>	TLS 1.1.												
	<i>tls-1.2</i>	TLS 1.2.												
<i>tls-1.3</i>	TLS 1.3.													
ssl-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable secure renegotiation.</td></tr><tr><td><i>disable</i></td><td>Disable secure renegotiation.</td></tr></table>	Option	Description	<i>enable</i>	Enable secure renegotiation.	<i>disable</i>	Disable secure renegotiation.							
	Option	Description												
	<i>enable</i>	Enable secure renegotiation.												
<i>disable</i>	Disable secure renegotiation.													
ssl-vpn-web-portal *	Agentless VPN web portal.	string	Maximum length: 35											
url-map	URL pattern to match.	string	Maximum length: 511	/										
url-map-type	Type of url-map.	option	-	sub-string										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sub-string</i></td><td>Match the pattern if a string contains the sub-string.</td></tr><tr><td><i>wildcard</i></td><td>Match the pattern with wildcards.</td></tr><tr><td><i>regex</i></td><td>Match the pattern with a regular expression.</td></tr></table>	Option	Description	<i>sub-string</i>	Match the pattern if a string contains the sub-string.	<i>wildcard</i>	Match the pattern with wildcards.	<i>regex</i>	Match the pattern with a regular expression.					
	Option	Description												
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.												
	<i>wildcard</i>	Match the pattern with wildcards.												
<i>regex</i>	Match the pattern with a regular expression.													
virtual-host	Virtual host.	string	Maximum length: 79											

* This parameter may not exist in some models.

config quic

Parameter	Description	Type	Size	Default						
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3						
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2						
active-migration	Enable/disable active migration (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable active migration.</td></tr><tr><td><i>disable</i></td><td>Disable active migration.</td></tr></table>	Option	Description	<i>enable</i>	Enable active migration.	<i>disable</i>	Disable active migration.			
Option	Description									
<i>enable</i>	Enable active migration.									
<i>disable</i>	Disable active migration.									
grease-quic-bit	Enable/disable grease QUIC bit (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable grease QUIC bit.</td></tr><tr><td><i>disable</i></td><td>Disable grease QUIC bit.</td></tr></table>	Option	Description	<i>enable</i>	Enable grease QUIC bit.	<i>disable</i>	Disable grease QUIC bit.			
Option	Description									
<i>enable</i>	Enable grease QUIC bit.									
<i>disable</i>	Disable grease QUIC bit.									
max-ack-delay	Maximum ACK delay in milliseconds (1 - 16383, default = 25).	integer	Minimum value: 1 Maximum value: 16383	25						
max-datagram-frame-size	Maximum datagram frame size in bytes (1 - 1500, default = 1500).	integer	Minimum value: 1 Maximum value: 1500	1500						
max-idle-timeout	Maximum idle timeout milliseconds (1 - 60000, default = 30000).	integer	Minimum value: 1 Maximum value: 60000	30000						
max-udp-payload-size	Maximum UDP payload size in bytes (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500						

config realservers

Parameter	Description	Type	Size	Default								
addr-type	Type of address.	option	-	ip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ip</td><td>Standard IPv4 address.</td></tr><tr><td>fqdn</td><td>Non-wildcard FQDN address object.</td></tr></table>	Option	Description	ip	Standard IPv4 address.	fqdn	Non-wildcard FQDN address object.					
Option	Description											
ip	Standard IPv4 address.											
fqdn	Non-wildcard FQDN address object.											
address	Address or address group of the real server.	string	Maximum length: 79									
domain	Wildcard domain name of the real server.	string	Maximum length: 255									
external-auth	Enable/disable use of external browser as user-agent for SAML user authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of external browser as user-agent for SAML user authentication.</td></tr><tr><td>disable</td><td>Disable use of external browser as user-agent for SAML user authentication.</td></tr></table>	Option	Description	enable	Enable use of external browser as user-agent for SAML user authentication.	disable	Disable use of external browser as user-agent for SAML user authentication.					
Option	Description											
enable	Enable use of external browser as user-agent for SAML user authentication.											
disable	Disable use of external browser as user-agent for SAML user authentication.											
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable per server health check.</td></tr><tr><td>enable</td><td>Enable per server health check.</td></tr></table>	Option	Description	disable	Disable per server health check.	enable	Enable per server health check.					
Option	Description											
disable	Disable per server health check.											
enable	Enable per server health check.											
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>Use PING to test the link with the server.</td></tr><tr><td>http</td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td>tcp-connect</td><td>Use a full TCP connection to test the link with the server.</td></tr></table>	Option	Description	ping	Use PING to test the link with the server.	http	Use HTTP-GET to test the link with the server.	tcp-connect	Use a full TCP connection to test the link with the server.			
Option	Description											
ping	Use PING to test the link with the server.											
http	Use HTTP-GET to test the link with the server.											
tcp-connect	Use a full TCP connection to test the link with the server.											
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per server holddown.</td></tr><tr><td><i>disable</i></td><td>Disable per server holddown.</td></tr></table>	Option	Description	<i>enable</i>	Enable per server holddown.	<i>disable</i>	Disable per server holddown.					
	Option	Description										
	<i>enable</i>	Enable per server holddown.										
<i>disable</i>	Disable per server holddown.											
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
id	Real server ID.	integer	Minimum value: 0 0 Maximum value: 4294967295									
ip	IP address of the real server.	ipv4-address-any	Not Specified	0.0.0.0								
mappedport	Port for communicating with the real server.	user	Not Specified									
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79									
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79									
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSH real server host key validation.</td></tr><tr><td><i>enable</i></td><td>Enable SSH real server host key validation.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSH real server host key validation.	<i>enable</i>	Enable SSH real server host key validation.					
	Option	Description										
	<i>disable</i>	Disable SSH real server host key validation.										
<i>enable</i>	Enable SSH real server host key validation.											
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Server status active.</td></tr><tr><td><i>standby</i></td><td>Server status standby.</td></tr><tr><td><i>disable</i></td><td>Server status disable.</td></tr></table>	Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.			
	Option	Description										
	<i>active</i>	Server status active.										
	<i>standby</i>	Server status standby.										
<i>disable</i>	Server status disable.											
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable virtual hostname/IP translation.		
	<i>disable</i>	Disable virtual hostname/IP translation.		
tunnel-encryption	Tunnel encryption.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp forwarding tunnel encryption.		
	<i>disable</i>	Disable tcp forwarding tunnel encryption.		
type	TCP forwarding server type.	option	-	tcp-forwarding
	Option	Description		
	<i>tcp-forwarding</i>	TCP forwarding.		
	<i>ssh</i>	SSH.		
verify-cert	Enable/disable certificate verification of the real server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable certificate verification.		
	<i>disable</i>	Disable certificate verification.		
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	
	Option	Description		
	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.		
	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr></table>	Option	Description	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.			
Option	Description																									
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.																									
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																									
<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.																									
<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																									
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																									
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																									

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.</td></tr></table>	Option	Description	TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.			
Option	Description																									
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																									
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																									
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																									
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.																									
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.																									
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.																									
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.																									
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.																									
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.																									
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.																									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.			
Option	Description																							
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																							
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.																							
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.																							
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.																							
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.																							
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.																							
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.																							
<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.																							
<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.																							

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.			
Option	Description																									
<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																									
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.																									

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																								
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																								
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																								
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																								
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																								
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																								
<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																									
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																									
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295																							

Parameter	Description	Type	Size	Default
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3
	Option Description			
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config api-gateway6

Parameter	Description	Type	Size	Default
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79	
h2-support	HTTP2 support, default=Enable.	option	-	enable
	Option Description			
	<i>enable</i>	Enable HTTP2 support.		
	<i>disable</i>	Disable HTTP2 support.		
h3-support	HTTP3/QUIC support, default=Disable.	option	-	disable
	Option Description			
	<i>enable</i>	Enable HTTP3/QUIC support.		
	<i>disable</i>	Disable HTTP3/QUIC support.		
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 60 0 Maximum value: 525600	
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).		
	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.		
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35	
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	Option	Description		
	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.		
	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.		
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.		
	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.		
id	API Gateway ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option	Description		
	<i>static</i>	Distribute to server based on source IP.		
	<i>round-robin</i>	Distribute to server based round robin order.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weighted</i></td><td>Distribute to server based on weight.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	<i>weighted</i>	Distribute to server based on weight.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.									
	Option	Description																
	<i>weighted</i>	Distribute to server based on weight.																
	<i>first-alive</i>	Distribute to the first server that is alive.																
<i>http-host</i>	Distribute to server based on host field in HTTP header.																	
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.											
	Option	Description																
	<i>none</i>	None.																
<i>http-cookie</i>	HTTP cookie.																	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not support redirection after successful SAML authentication.</td></tr><tr><td><i>enable</i></td><td>Support redirection after successful SAML authentication.</td></tr></table>	Option	Description	<i>disable</i>	Do not support redirection after successful SAML authentication.	<i>enable</i>	Support redirection after successful SAML authentication.											
	Option	Description																
	<i>disable</i>	Do not support redirection after successful SAML authentication.																
<i>enable</i>	Support redirection after successful SAML authentication.																	
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35															
service	Service.	option	-	https														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>tcp-forwarding</i></td><td>TCP-FORWARDING.</td></tr><tr><td><i>samlsp</i></td><td>SAML-SP.</td></tr><tr><td><i>web-portal</i></td><td>VPN-SSL-WEB-PORTAL.</td></tr><tr><td><i>saas</i></td><td>SAAS.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.	<i>tcp-forwarding</i>	TCP-FORWARDING.	<i>samlsp</i>	SAML-SP.	<i>web-portal</i>	VPN-SSL-WEB-PORTAL.	<i>saas</i>	SAAS.			
	Option	Description																
	<i>http</i>	HTTP.																
	<i>https</i>	HTTPS.																
	<i>tcp-forwarding</i>	TCP-FORWARDING.																
	<i>samlsp</i>	SAML-SP.																
	<i>web-portal</i>	VPN-SSL-WEB-PORTAL.																
<i>saas</i>	SAAS.																	
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.													
	Option	Description																
<i>high</i>	High encryption. Allow only AES and ChaCha.																	

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											
	Option	Description																
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td><i>3072</i></td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td><i>4096</i></td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.			
	Option	Description																
	<i>768</i>	768-bit Diffie-Hellman prime.																
	<i>1024</i>	1024-bit Diffie-Hellman prime.																
	<i>1536</i>	1536-bit Diffie-Hellman prime.																
	<i>2048</i>	2048-bit Diffie-Hellman prime.																
	<i>3072</i>	3072-bit Diffie-Hellman prime.																
<i>4096</i>	4096-bit Diffie-Hellman prime.																	
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																	
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																	
ssl-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable secure renegotiation.		
	<i>disable</i>	Disable secure renegotiation.		
ssl-vpn-web-portal *	Agentless VPN web portal.	string	Maximum length: 35	
url-map	URL pattern to match.	string	Maximum length: 511	/
url-map-type	Type of url-map.	option	-	sub-string
	Option	Description		
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.		
	<i>wildcard</i>	Match the pattern with wildcards.		
	<i>regex</i>	Match the pattern with a regular expression.		
virtual-host	Virtual host.	string	Maximum length: 79	

* This parameter may not exist in some models.

config quic

Parameter	Description	Type	Size	Default						
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3						
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2						
active-migration	Enable/disable active migration (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable active migration.</td></tr><tr><td><i>disable</i></td><td>Disable active migration.</td></tr></table>				Option	Description	<i>enable</i>	Enable active migration.	<i>disable</i>	Disable active migration.
Option	Description									
<i>enable</i>	Enable active migration.									
<i>disable</i>	Disable active migration.									
grease-quic-bit	Enable/disable grease QUIC bit (default = enable).	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable grease QUIC bit.		
	<i>disable</i>	Disable grease QUIC bit.		
max-ack-delay	Maximum ACK delay in milliseconds (1 - 16383, default = 25).	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes (1 - 1500, default = 1500).	integer	Minimum value: 1 Maximum value: 1500	1500
max-idle-timeout	Maximum idle timeout milliseconds (1 - 60000, default = 30000).	integer	Minimum value: 1 Maximum value: 60000	30000
max-udp-payload-size	Maximum UDP payload size in bytes (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500

config realservers

Parameter	Description	Type	Size	Default						
addr-type	Type of address.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Non-wildcard FQDN address object.</td></tr></table>				Option	Description	<i>ip</i>	Standard IPv4 address.	<i>fqdn</i>	Non-wildcard FQDN address object.
	Option	Description								
	<i>ip</i>	Standard IPv4 address.								
<i>fqdn</i>	Non-wildcard FQDN address object.									
address	Address or address group of the real server.	string	Maximum length: 79							
domain	Wildcard domain name of the real server.	string	Maximum length: 255							
external-auth	Enable/disable use of external browser as user-agent for SAML user authentication.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of external browser as user-agent for SAML user authentication.</td></tr><tr><td><i>disable</i></td><td>Disable use of external browser as user-agent for SAML user authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of external browser as user-agent for SAML user authentication.	<i>disable</i>	Disable use of external browser as user-agent for SAML user authentication.					
	Option	Description										
	<i>enable</i>	Enable use of external browser as user-agent for SAML user authentication.										
<i>disable</i>	Disable use of external browser as user-agent for SAML user authentication.											
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr></table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.					
	Option	Description										
	<i>disable</i>	Disable per server health check.										
<i>enable</i>	Enable per server health check.											
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>Use PING to test the link with the server.</td></tr><tr><td><i>http</i></td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td><i>tcp-connect</i></td><td>Use a full TCP connection to test the link with the server.</td></tr></table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.			
	Option	Description										
	<i>ping</i>	Use PING to test the link with the server.										
	<i>http</i>	Use HTTP-GET to test the link with the server.										
<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.											
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per server holddown.</td></tr><tr><td><i>disable</i></td><td>Disable per server holddown.</td></tr></table>	Option	Description	<i>enable</i>	Enable per server holddown.	<i>disable</i>	Disable per server holddown.					
	Option	Description										
	<i>enable</i>	Enable per server holddown.										
<i>disable</i>	Disable per server holddown.											
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295									
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::								
mappedport	Port for communicating with the real server.	user	Not Specified									

Parameter	Description	Type	Size	Default								
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79									
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79									
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SSH real server host key validation.</td></tr><tr><td>enable</td><td>Enable SSH real server host key validation.</td></tr></table>				Option	Description	disable	Disable SSH real server host key validation.	enable	Enable SSH real server host key validation.		
Option	Description											
disable	Disable SSH real server host key validation.											
enable	Enable SSH real server host key validation.											
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>active</td><td>Server status active.</td></tr><tr><td>standby</td><td>Server status standby.</td></tr><tr><td>disable</td><td>Server status disable.</td></tr></table>				Option	Description	active	Server status active.	standby	Server status standby.	disable	Server status disable.
Option	Description											
active	Server status active.											
standby	Server status standby.											
disable	Server status disable.											
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable virtual hostname/IP translation.</td></tr><tr><td>disable</td><td>Disable virtual hostname/IP translation.</td></tr></table>				Option	Description	enable	Enable virtual hostname/IP translation.	disable	Disable virtual hostname/IP translation.		
Option	Description											
enable	Enable virtual hostname/IP translation.											
disable	Disable virtual hostname/IP translation.											
tunnel-encryption	Tunnel encryption.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable tcp forwarding tunnel encryption.</td></tr><tr><td>disable</td><td>Disable tcp forwarding tunnel encryption.</td></tr></table>				Option	Description	enable	Enable tcp forwarding tunnel encryption.	disable	Disable tcp forwarding tunnel encryption.		
Option	Description											
enable	Enable tcp forwarding tunnel encryption.											
disable	Disable tcp forwarding tunnel encryption.											
type	TCP forwarding server type.	option	-	tcp-forwarding								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tcp-forwarding</i>	TCP forwarding.		
	<i>ssh</i>	SSH.		
verify-cert	Enable/disable certificate verification of the real server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable certificate verification.		
	<i>disable</i>	Disable certificate verification.		
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default												
cipher	Cipher suite name.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr></table>				Option	Description	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
Option	Description															
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.															
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.															
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.															
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.															
<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.															

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.			
Option	Description																											
<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																											
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																											
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																											
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																											
<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																											
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																											
<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																											
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																											
<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																											
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																											
<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	TLS-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
TLS-ECDHE-RSA-WITH-RC4-128-SHA	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.		
	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.		
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295	
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3
	Option	Description		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config firewall access-proxy-ssh-client-cert

Configure Access Proxy SSH client certificate.

```
config firewall access-proxy-ssh-client-cert
  Description: Configure Access Proxy SSH client certificate.
  edit <name>
    set auth-ca {string}
    config cert-extension
      Description: Configure certificate extension for user certificate.
      edit <name>
        set critical [no|yes]
        set data {string}
        set type [fixed|user]
      next
    end
    set permit-agent-forwarding [enable|disable]
    set permit-port-forwarding [enable|disable]
    set permit-pty [enable|disable]
    set permit-user-rc [enable|disable]
    set permit-x11-forwarding [enable|disable]
    set source-address [enable|disable]
  next
end
```

config firewall access-proxy-ssh-client-cert

Parameter	Description	Type	Size	Default						
auth-ca	Name of the SSH server public key authentication CA.	string	Maximum length: 79							
name	SSH client certificate name.	string	Maximum length: 79							
permit-agent-forwarding	Enable/disable appending permit-agent-forwarding certificate extension.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
permit-port-forwarding	Enable/disable appending permit-port-forwarding certificate extension.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-pty	Enable/disable appending permit-pty certificate extension.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-user-rc	Enable/disable appending permit-user-rc certificate extension.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-x11-forwarding	Enable/disable appending permit-x11-forwarding certificate extension.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
source-address	Enable/disable appending source-address certificate critical option. This option ensure certificate only accepted from FortiGate source address.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config cert-extension

Parameter	Description	Type	Size	Default
critical	Critical option.	option	-	no

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>no</i>	Certificate extension, server ignores the unsupported certificate extension.		
	<i>yes</i>	Critical option, server refuses to authorize if it cannot recognize the critical option.		
data	Data of certificate extension.	string	Maximum length: 127	
name	Name of certificate extension.	string	Maximum length: 127	
type	Type of certificate extension.	option	-	fixed
	Option	Description		
	<i>fixed</i>	Fixed certificate extension entry.		
	<i>user</i>	Certificate extension entry filled with authenticated username.		

config firewall access-proxy-virtual-host

Configure Access Proxy virtual hosts.

```
config firewall access-proxy-virtual-host
  Description: Configure Access Proxy virtual hosts.
  edit <name>
    set client-cert [disable|enable]
    set empty-cert-action [accept|block|...]
    set host {string}
    set host-type [sub-string|wildcard]
    set replacemsg-group {string}
    set ssl-certificate <name1>, <name2>, ...
    set user-agent-detect [disable|enable]
  next
end
```

config firewall access-proxy-virtual-host

Parameter	Description	Type	Size	Default
client-cert	Enable/disable requesting client certificate.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable client certificate request.		
	<i>enable</i>	Enable client certificate request.		
empty-cert-action	Action for an empty client certificate.	option	-	block
	Option	Description		
	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.		
	<i>block</i>	Block the SSL handshake if the client certificate is empty.		
	<i>accept-unmanageable</i>	Accept the SSL handshake only if the end-point is unmanageable.		
host	The host name.	string	Maximum length: 79	
host-type	Type of host pattern.	option	-	sub-string
	Option	Description		
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.		
	<i>wildcard</i>	Match the pattern with wildcards.		
name	Virtual host name.	string	Maximum length: 79	
replacemsg-group	Access-proxy-virtual-host replacement message override group.	string	Maximum length: 35	
ssl-certificate <name>	SSL certificates for this host. Certificate list.	string	Maximum length: 79	
user-agent-detect	Enable/disable detecting device type by HTTP user-agent if no client certificate is provided.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable detecting unknown devices by HTTP user-agent if no client certificate is provided.		
	<i>enable</i>	Enable detecting unknown devices by HTTP user-agent if no client certificate is provided.		

config firewall acl



This command is available for model(s): FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200F, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 900G, FortiGate 901G.

It is not available for: FortiGate 1000D, FortiGate 200E, FortiGate 201E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure IPv4 access control list.

```
config firewall acl
  Description: Configure IPv4 access control list.
  edit <policyid>
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set fragment [pass|drop]
    set interface {string}
    set name {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
  next
end
```

config firewall acl

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 1023							
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79							
fragment	Pass/drop fragments that match L3 information.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pass</td><td>Pass fragments that match interface, srcaddr, and dstaddr.</td></tr><tr><td>drop</td><td>Drop fragments that match interface, srcaddr, and dstaddr.</td></tr></table>				Option	Description	pass	Pass fragments that match interface, srcaddr, and dstaddr.	drop	Drop fragments that match interface, srcaddr, and dstaddr.
Option	Description									
pass	Pass fragments that match interface, srcaddr, and dstaddr.									
drop	Drop fragments that match interface, srcaddr, and dstaddr.									
interface	Interface name.	string	Maximum length: 35							
name	Policy name.	string	Maximum length: 35							
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999	0						
service <name>	Service name. Service name.	string	Maximum length: 79							
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79							
status	Enable/disable access control list status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable access control list status.</td></tr><tr><td>disable</td><td>Disable access control list status.</td></tr></table>				Option	Description	enable	Enable access control list status.	disable	Disable access control list status.
Option	Description									
enable	Enable access control list status.									
disable	Disable access control list status.									

config firewall acl6



This command is available for model(s): FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200F, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 900G, FortiGate 901G.

It is not available for: FortiGate 1000D, FortiGate 200E, FortiGate 201E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure IPv6 access control list.

```
config firewall acl6
  Description: Configure IPv6 access control list.
  edit <policyid>
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set fragment [pass|drop]
    set interface {string}
    set name {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
  next
end
```

config firewall acl6

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 1023							
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79							
fragment	Pass/drop fragments that match L3 information.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pass</td><td>Pass fragments that match interface, srcaddr, and dstaddr.</td></tr><tr><td>drop</td><td>Drop fragments that match interface, srcaddr, and dstaddr.</td></tr></table>	Option	Description	pass	Pass fragments that match interface, srcaddr, and dstaddr.	drop	Drop fragments that match interface, srcaddr, and dstaddr.			
Option	Description									
pass	Pass fragments that match interface, srcaddr, and dstaddr.									
drop	Drop fragments that match interface, srcaddr, and dstaddr.									
interface	Interface name.	string	Maximum length: 35							
name	Policy name.	string	Maximum length: 35							
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999	0						
service <name>	Service name. Service name.	string	Maximum length: 79							
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79							
status	Enable/disable access control list status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable access control list status.</td></tr><tr><td>disable</td><td>Disable access control list status.</td></tr></table>	Option	Description	enable	Enable access control list status.	disable	Disable access control list status.			
Option	Description									
enable	Enable access control list status.									
disable	Disable access control list status.									

config firewall address

Configure IPv4 addresses.

```
config firewall address
  Description: Configure IPv4 addresses.
  edit <name>
    set allow-routing [enable|disable]
```

```

set associated-interface {string}
set cache-ttl {integer}
set clearpass-spt [unknown|healthy|...]
set color {integer}
set comment {var-string}
set country {string}
set end-ip {ipv4-address-any}
set epg-name {string}
set fabric-object [enable|disable]
set filter {var-string}
set fqdn {string}
set fsso-group <name1>, <name2>, ...
set hw-model {string}
set hw-vendor {string}
set interface {string}
config list
    Description: IP address list.
    edit <ip>
    next
end
set macaddr <macaddr1>, <macaddr2>, ...
set node-ip-only [enable|disable]
set obj-id {var-string}
set obj-tag {string}
set obj-type [ip|mac]
set organization {string}
set os {string}
set policy-group {string}
set route-tag {integer}
set sdn {string}
set sdn-addr-type [private|public|...]
set sdn-tag {string}
set sso-attribute-value <name1>, <name2>, ...
set start-ip {ipv4-address-any}
set sub-type [sdn|clearpass-spt|...]
set subnet {ipv4-classnet-any}
set subnet-name {string}
set sw-version {string}
set tag-detection-level {string}
set tag-type {string}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set tenant {string}
set type [ipmask|iprange|...]
set uuid {uuid}
set wildcard {ipv4-classnet-any}
set wildcard-fqdn {string}

```

```
next
end
```

config firewall address

Parameter	Description	Type	Size	Default
allow-routing	Enable/disable use of this address in routing configurations.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of this address in routing configurations.		
	<i>disable</i>	Disable use of this address in routing configurations.		
associated-interface	Network interface associated with address.	string	Maximum length: 35	
cache-ttl	Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds.	integer	Minimum value: 0 0 Maximum value: 86400	
clearpass-spt	SPT (System Posture Token) value.	option	-	unknown
	Option	Description		
	<i>unknown</i>	UNKNOWN.		
	<i>healthy</i>	HEALTHY.		
	<i>quarantine</i>	QUARANTINE.		
	<i>checkup</i>	CHECKUP.		
	<i>transient</i>	TRANSIENT.		
	<i>infected</i>	INFECTED.		
color	Color of icon on the GUI.	integer	Minimum value: 0 0 Maximum value: 32	
comment	Comment.	var-string	Maximum length: 255	
country	IP addresses associated to a specific country.	string	Maximum length: 2	
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
epg-name	Endpoint group name.	string	Maximum length: 255							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td>disable</td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	enable	Object is set as a security fabric-wide global object.	disable	Object is local to this security fabric member.
Option	Description									
enable	Object is set as a security fabric-wide global object.									
disable	Object is local to this security fabric member.									
filter	Match criteria filter.	var-string	Maximum length: 2047							
fqdn	Fully Qualified Domain Name address.	string	Maximum length: 255							
fsso-group <name>	FSSO group(s). FSSO group name.	string	Maximum length: 511							
hw-model	Dynamic address matching hardware model.	string	Maximum length: 35							
hw-vendor	Dynamic address matching hardware vendor.	string	Maximum length: 35							
interface	Name of interface whose IP address is to be used.	string	Maximum length: 35							
macaddr <macaddr>	Multiple MAC address ranges. MAC address ranges <start>[-<end>] separated by space.	string	Maximum length: 127							
name	Address name.	string	Maximum length: 79							
node-ip-only	Enable/disable collection of node addresses only in Kubernetes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable collection of node addresses only in Kubernetes.</td></tr><tr><td>disable</td><td>Disable collection of node addresses only in Kubernetes.</td></tr></table>				Option	Description	enable	Enable collection of node addresses only in Kubernetes.	disable	Disable collection of node addresses only in Kubernetes.
Option	Description									
enable	Enable collection of node addresses only in Kubernetes.									
disable	Disable collection of node addresses only in Kubernetes.									
obj-id	Object ID for NSX.	var-string	Maximum length: 255							
obj-tag	Tag of dynamic address object.	string	Maximum length: 255							
obj-type	Object type.	option	-	ip						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ip</i>	IP address.		
	<i>mac</i>	MAC address		
organization	Organization domain name (Syntax: organization/domain).	string	Maximum length: 35	
os	Dynamic address matching operating system.	string	Maximum length: 35	
policy-group	Policy group name.	string	Maximum length: 15	
route-tag	route-tag address.	integer	Minimum value: 0 1 Maximum value: 4294967295	
sdn	SDN.	string	Maximum length: 35	
sdn-addr-type	Type of addresses to collect.	option	-	private
	Option	Description		
	<i>private</i>	Collect private addresses only.		
	<i>public</i>	Collect public addresses only.		
	<i>all</i>	Collect both public and private addresses.		
sdn-tag	SDN Tag.	string	Maximum length: 15	
sso-attribute-value <name>	RADIUS attributes value. RADIUS attribute value.	string	Maximum length: 511	
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
sub-type	Sub-type of address.	option	-	sdn
	Option	Description		
	<i>sdn</i>	SDN address.		
	<i>clearpass-spt</i>	ClearPass SPT (System Posture Token) address.		
	<i>fsso</i>	FSSO address.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>rssso</i>	RSSO address.		
	<i>ems-tag</i>	FortiClient EMS tag.		
	<i>fortivoice-tag</i>	FortiVoice tag.		
	<i>fortinac-tag</i>	FortiNAC tag.		
	<i>swc-tag</i>	Switch Controller NAC policy tag.		
	<i>device-identification</i>	Device address.		
	<i>external-resource</i>	External resource.		
	<i>obsolete</i>	Tag from EOL product.		
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
subnet-name	Subnet name.	string	Maximum length: 255	
sw-version	Dynamic address matching software version.	string	Maximum length: 35	
tag-detection-level	Tag detection level of dynamic address object.	string	Maximum length: 15	
tag-type	Tag type of dynamic address object.	string	Maximum length: 63	
tenant	Tenant.	string	Maximum length: 35	
type	Type of address.	option	-	ipmask
	Option	Description		
	<i>ipmask</i>	Standard IPv4 address with subnet mask.		
	<i>iprange</i>	Range of IPv4 addresses between two specified addresses (inclusive).		
	<i>fqdn</i>	Fully Qualified Domain Name address.		
	<i>geography</i>	IP addresses from a specified country.		
	<i>wildcard</i>	Standard IPv4 using a wildcard subnet mask.		
	<i>dynamic</i>	Dynamic address object.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>interface-subnet</i>	IP and subnet of interface.		
	<i>mac</i>	Range of MAC addresses.		
	<i>route-tag</i>	route-tag addresses.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wildcard	IP address and wildcard netmask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.	string	Maximum length: 255	

config list

Parameter	Description	Type	Size	Default
ip	IP.	string	Maximum length: 35	

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall address6

Configure IPv6 firewall addresses.

```
config firewall address6
  Description: Configure IPv6 firewall addresses.
  edit <name>
    set cache-ttl {integer}
```

```

set color {integer}
set comment {var-string}
set country {string}
set end-ip {ipv6-address}
set epg-name {string}
set fabric-object [enable|disable]
set filter {var-string}
set fqdn {string}
set host {ipv6-address}
set host-type [any|specific]
set ip6 {ipv6-network}
config list
    Description: IP address list.
    edit <ip>
        next
    end
set macaddr <macaddr1>, <macaddr2>, ...
set obj-id {var-string}
set route-tag {integer}
set sdn {string}
set sdn-addr-type [private|public|...]
set sdn-tag {string}
set start-ip {ipv6-address}
config subnet-segment
    Description: IPv6 subnet segments.
    edit <name>
        set type [any|specific]
        set value {string}
    next
end
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set template {string}
set tenant {string}
set type [ipprefix|iprange|...]
set uuid {uuid}
next
end

```

config firewall address6

Parameter	Description	Type	Size	Default						
cache-ttl	Minimal TTL of individual IPv6 addresses in FQDN cache.	integer	Minimum value: 0 Maximum value: 86400	0						
color	Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32	0						
comment	Comment.	var-string	Maximum length: 255							
country	IPv6 addresses associated to a specific country.	string	Maximum length: 2							
end-ip	Final IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::						
epg-name	Endpoint group name.	string	Maximum length: 255							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									
filter	Match criteria filter.	var-string	Maximum length: 2047							
fqdn	Fully qualified domain name.	string	Maximum length: 255							
host	Host Address.	ipv6-address	Not Specified	::						
host-type	Host type.	option	-	any						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Wildcard.</td></tr><tr><td><i>specific</i></td><td>Specific host address.</td></tr></table>				Option	Description	<i>any</i>	Wildcard.	<i>specific</i>	Specific host address.
Option	Description									
<i>any</i>	Wildcard.									
<i>specific</i>	Specific host address.									

Parameter	Description	Type	Size	Default								
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xx x).	ipv6-network	Not Specified	::/0								
macaddr <macaddr>	Multiple MAC address ranges. MAC address ranges <start>[-<end>] separated by space.	string	Maximum length: 127									
name	Address name.	string	Maximum length: 79									
obj-id	Object ID for NSX.	var-string	Maximum length: 255									
route-tag	route-tag address.	integer	Minimum value: 1 Maximum value: 4294967295	0								
sdn	SDN.	string	Maximum length: 35									
sdn-addr-type	Type of addresses to collect.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>private</td><td>Collect private addresses only.</td></tr><tr><td>public</td><td>Collect public addresses only.</td></tr><tr><td>all</td><td>Collect both public and private addresses.</td></tr></table>				Option	Description	private	Collect private addresses only.	public	Collect public addresses only.	all	Collect both public and private addresses.
Option	Description											
private	Collect private addresses only.											
public	Collect public addresses only.											
all	Collect both public and private addresses.											
sdn-tag	SDN Tag.	string	Maximum length: 15									
start-ip	First IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::								
template	IPv6 address template.	string	Maximum length: 63									
tenant	Tenant.	string	Maximum length: 35									
type	Type of IPv6 address object (default = ipprefix).	option	-	ipprefix								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ipprefix</i>	Uses the IP prefix to define a range of IPv6 addresses.		
	<i>iprange</i>	Range of IPv6 addresses between two specified addresses (inclusive).		
	<i>fqdn</i>	Fully qualified domain name.		
	<i>geography</i>	IPv6 addresses from a specified country.		
	<i>dynamic</i>	Dynamic address object for SDN.		
	<i>template</i>	Template.		
	<i>mac</i>	Range of MAC addresses.		
	<i>route-tag</i>	route-tag addresses.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config list

Parameter	Description	Type	Size	Default
ip	IP.	string	Maximum length: 89	

config subnet-segment

Parameter	Description	Type	Size	Default						
name	Name.	string	Maximum length: 63							
type	Subnet segment type.	option	-	any						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>any</td><td>Wildcard.</td></tr><tr><td>specific</td><td>Specific subnet segment address.</td></tr></table>				Option	Description	any	Wildcard.	specific	Specific subnet segment address.
	Option	Description								
	any	Wildcard.								
specific	Specific subnet segment address.									
value	Subnet segment value.	string	Maximum length: 35							

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall address6-template

Configure IPv6 address templates.

```
config firewall address6-template
  Description: Configure IPv6 address templates.
  edit <name>
    set fabric-object [enable|disable]
    set ip6 {ipv6-network}
    config subnet-segment
      Description: IPv6 subnet segments.
      edit <id>
        set bits {integer}
        set exclusive [enable|disable]
        set name {string}
        config values
          Description: Subnet segment values.
          edit <name>
            set value {string}
          next
        end
      next
    end
  set subnet-segment-count {integer}
  set uuid {uuid}
next
end
```

config firewall address6-template

Parameter	Description	Type	Size	Default
fabric-object	Security Fabric global object setting.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		
ip6	IPv6 address prefix.	ipv6-network	Not Specified	::/0
name	IPv6 address template name.	string	Maximum length: 63	
subnet-segment-count	Number of IPv6 subnet segments.	integer	Minimum value: 1 Maximum value: 6	0
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config subnet-segment

Parameter	Description	Type	Size	Default
bits	Number of bits.	integer	Minimum value: 0 1 Maximum value: 16	0
exclusive	Enable/disable exclusive value.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable exclusive value.		
	<i>disable</i>	Disable exclusive value.		
id	Subnet segment ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
name	Subnet segment name.	string	Maximum length: 63	

config values

Parameter	Description	Type	Size	Default
name	Subnet segment value name.	string	Maximum length: 63	
value	Subnet segment value.	string	Maximum length: 35	

config firewall addrgrp

Configure IPv4 address groups.

```
config firewall addrgrp
  Description: Configure IPv4 address groups.
  edit <name>
    set allow-routing [enable|disable]
    set category [default|ztna-ems-tag|...]
    set color {integer}
    set comment {var-string}
    set exclude [enable|disable]
    set exclude-member <name1>, <name2>, ...
    set fabric-object [enable|disable]
    set member <name1>, <name2>, ...
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set type [default|folder]
    set uuid {uuid}
  next
end
```

config firewall addrgrp

Parameter	Description	Type	Size	Default
allow-routing	Enable/disable use of this group in routing configurations.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of this group in routing configurations.		
	<i>disable</i>	Disable use of this group in routing configurations.		

Parameter	Description	Type	Size	Default
category	Address group category.	option	-	default
	Option	Description		
	default	Default address group category (cannot be used as ztna-ems-tag/ztna-geo-tag in policy).		
	ztna-ems-tag	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.		
	ztna-geo-tag	Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
exclude	Enable/disable address exclusion.	option	-	disable
	Option	Description		
	enable	Enable address exclusion.		
	disable	Disable address exclusion.		
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79	
fabric-object	Security Fabric global object setting.	option	-	disable
	Option	Description		
	enable	Object is set as a security fabric-wide global object.		
	disable	Object is local to this security fabric member.		
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79	
name	Address group name.	string	Maximum length: 79	
type	Address group type.	option	-	default
	Option	Description		
	default	Default address group type (address may belong to multiple groups).		
	folder	Address folder group (members may not belong to any other group).		

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall addrgrp6

Configure IPv6 address groups.

```

config firewall addrgrp6
  Description: Configure IPv6 address groups.
  edit <name>
    set color {integer}
    set comment {var-string}
    set exclude [enable|disable]
    set exclude-member <name1>, <name2>, ...
    set fabric-object [enable|disable]
    set member <name1>, <name2>, ...
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set uuid {uuid}
  next
end

```

config firewall addrgrp6

Parameter	Description	Type	Size	Default						
color	Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32	0						
comment	Comment.	var-string	Maximum length: 255							
exclude	Enable/disable address6 exclusion.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable address6 exclusion.</td></tr><tr><td>disable</td><td>Disable address6 exclusion.</td></tr></table>				Option	Description	enable	Enable address6 exclusion.	disable	Disable address6 exclusion.
Option	Description									
enable	Enable address6 exclusion.									
disable	Disable address6 exclusion.									
exclude-member <name>	Address6 exclusion member. Address6 name.	string	Maximum length: 79							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td>disable</td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	enable	Object is set as a security fabric-wide global object.	disable	Object is local to this security fabric member.
Option	Description									
enable	Object is set as a security fabric-wide global object.									
disable	Object is local to this security fabric member.									
member <name>	Address objects contained within the group. Address6/addrgrp6 name.	string	Maximum length: 79							
name	IPv6 address group name.	string	Maximum length: 79							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall auth-portal

Configure firewall authentication portals.

```
config firewall auth-portal
  Description: Configure firewall authentication portals.
  set groups <name1>, <name2>, ...
  set identity-based-route {string}
  set portal-addr {string}
  set portal-addr6 {string}
  set proxy-auth [enable|disable]
end
```

config firewall auth-portal

Parameter	Description	Type	Size	Default
groups <name>	Firewall user groups permitted to authenticate through this portal. Separate group names with spaces. Group name.	string	Maximum length: 79	
identity-based-route	Name of the identity-based route that applies to this portal.	string	Maximum length: 35	
portal-addr	Address (or FQDN) of the authentication portal.	string	Maximum length: 63	
portal-addr6	IPv6 address (or FQDN) of authentication portal.	string	Maximum length: 63	
proxy-auth	Enable/disable authentication by proxy daemon (default = disable).	option	-	disable
		Option	Description	
		<i>enable</i>	Users are authenticated by proxy daemon.	
		<i>disable</i>	Users are not authenticated by proxy daemon.	

config firewall central-snat-map

Configure IPv4 and IPv6 central SNAT policies.

```
config firewall central-snat-map
  Description: Configure IPv4 and IPv6 central SNAT policies.
  edit <policyid>
    set comments {var-string}
    set dst-addr <name1>, <name2>, ...
```

```

set dst-addr6 <name1>, <name2>, ...
set dst-port {user}
set dstintf <name1>, <name2>, ...
set nat [disable|enable]
set nat-ippool <name1>, <name2>, ...
set nat-ippool6 <name1>, <name2>, ...
set nat-port {user}
set nat46 [enable|disable]
set nat64 [enable|disable]
set orig-addr <name1>, <name2>, ...
set orig-addr6 <name1>, <name2>, ...
set orig-port {user}
set port-preserve [enable|disable]
set port-random [enable|disable]
set protocol {integer}
set srcintf <name1>, <name2>, ...
set status [enable|disable]
set type [ipv4|ipv6]
set uuid {uuid}

next
end

```

config firewall central-snat-map

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 1023							
dst-addr <name>	IPv4 Destination address. Address name.	string	Maximum length: 79							
dst-addr6 <name>	IPv6 Destination address. Address name.	string	Maximum length: 79							
dst-port	Destination port or port range (1 to 65535, 0 means any port).	user	Not Specified							
dstintf <name>	Destination interface name from available interfaces. Interface name.	string	Maximum length: 79							
nat	Enable/disable source NAT.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable source NAT.</td></tr><tr><td>enable</td><td>Enable source NAT.</td></tr></table>				Option	Description	disable	Disable source NAT.	enable	Enable source NAT.
Option	Description									
disable	Disable source NAT.									
enable	Enable source NAT.									

Parameter	Description	Type	Size	Default						
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79							
nat-ippool6 <name>	IPv6 pools to be used for source NAT. IPv6 pool name.	string	Maximum length: 79							
nat-port	Translated port or port range (1 to 65535, 0 means any port).	user	Not Specified							
nat46	Enable/disable NAT46.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NAT46.</td></tr><tr><td>disable</td><td>Disable NAT46.</td></tr></table>				Option	Description	enable	Enable NAT46.	disable	Disable NAT46.
Option	Description									
enable	Enable NAT46.									
disable	Disable NAT46.									
nat64	Enable/disable NAT64.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NAT64.</td></tr><tr><td>disable</td><td>Disable NAT64.</td></tr></table>				Option	Description	enable	Enable NAT64.	disable	Disable NAT64.
Option	Description									
enable	Enable NAT64.									
disable	Disable NAT64.									
orig-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79							
orig-addr6 <name>	IPv6 Original address. Address name.	string	Maximum length: 79							
orig-port	Original TCP port (1 to 65535, 0 means any port).	user	Not Specified							
policyid	Policy ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
port-preserve	Enable/disable preservation of the original source port from source NAT if it has not been used.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Use the original source port if it has not been used.</td></tr><tr><td>disable</td><td>Source NAT always changes the source port.</td></tr></table>				Option	Description	enable	Use the original source port if it has not been used.	disable	Source NAT always changes the source port.
Option	Description									
enable	Use the original source port if it has not been used.									
disable	Source NAT always changes the source port.									

Parameter	Description	Type	Size	Default						
port-random	Enable/disable random source port selection for source NAT.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable random source port selection for source NAT.</td></tr><tr><td><i>disable</i></td><td>Disable random source port selection for source NAT.</td></tr></table>	Option	Description	<i>enable</i>	Enable random source port selection for source NAT.	<i>disable</i>	Disable random source port selection for source NAT.			
Option	Description									
<i>enable</i>	Enable random source port selection for source NAT.									
<i>disable</i>	Disable random source port selection for source NAT.									
protocol	Integer value for the protocol type (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0						
srcintf <name>	Source interface name from available interfaces. Interface name.	string	Maximum length: 79							
status	Enable/disable the active status of this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.			
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
type	IPv4/IPv6 source NAT.	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>Perform IPv4 source NAT.</td></tr><tr><td><i>ipv6</i></td><td>Perform IPv6 source NAT.</td></tr></table>	Option	Description	<i>ipv4</i>	Perform IPv4 source NAT.	<i>ipv6</i>	Perform IPv6 source NAT.			
Option	Description									
<i>ipv4</i>	Perform IPv4 source NAT.									
<i>ipv6</i>	Perform IPv6 source NAT.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

config firewall city

Define city table. Read-only.

```
config firewall city
    Description: Define city table. Read-only.
    edit <id>
        set name {string}
    next
end
```

config firewall city

Parameter	Description	Type	Size	Default
id	City ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	City name.	string	Maximum length: 63	

config firewall country

Define country table. Read-only.

```
config firewall country
  Description: Define country table. Read-only.
  edit <id>
    set name {string}
    set region <id1>, <id2>, ...
  next
end
```

config firewall country

Parameter	Description	Type	Size	Default
id	Country ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	Country name.	string	Maximum length: 63	
region <id>	Region ID list. Region ID.	integer	Minimum value: 0 Maximum value: 65535	

config firewall decrypted-traffic-mirror

Configure decrypted traffic mirror.

```
config firewall decrypted-traffic-mirror
  Description: Configure decrypted traffic mirror.
  edit <name>
    set dstmac {mac-address}
    set interface <name1>, <name2>, ...
    set traffic-source [client|server|...]
    set traffic-type {option1}, {option2}, ...
  next
end
```

config firewall decrypted-traffic-mirror

Parameter	Description	Type	Size	Default								
dstmac	Set destination MAC address for mirrored traffic.	mac-address	Not Specified	ff:ff:ff:ff:ff:ff								
interface <name>	Decrypted traffic mirror interface. Decrypted traffic mirror interface.	string	Maximum length: 79									
name	Name.	string	Maximum length: 35									
traffic-source	Source of decrypted traffic to be mirrored.	option	-	client								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>client</td><td>Mirror client side decrypted traffic.</td></tr><tr><td>server</td><td>Mirror server side decrypted traffic.</td></tr><tr><td>both</td><td>Mirror both client and server side decrypted traffic.</td></tr></table>				Option	Description	client	Mirror client side decrypted traffic.	server	Mirror server side decrypted traffic.	both	Mirror both client and server side decrypted traffic.
Option	Description											
client	Mirror client side decrypted traffic.											
server	Mirror server side decrypted traffic.											
both	Mirror both client and server side decrypted traffic.											
traffic-type	Types of decrypted traffic to be mirrored.	option	-	ssl								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl</td><td>Mirror decrypted SSL traffic.</td></tr><tr><td>ssh</td><td>Mirror decrypted SSH traffic.</td></tr></table>				Option	Description	ssl	Mirror decrypted SSL traffic.	ssh	Mirror decrypted SSH traffic.		
Option	Description											
ssl	Mirror decrypted SSL traffic.											
ssh	Mirror decrypted SSH traffic.											

config firewall dnstranslation

Configure DNS translation.

```

config firewall dnstranslation
    Description: Configure DNS translation.
    edit <id>
        set dst {ipv4-address}
        set netmask {ipv4-netmask}
        set src {ipv4-address}
    next
end

```

config firewall dnstranslation

Parameter	Description	Type	Size	Default
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified	255.255.255.255
src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified	0.0.0.0

config firewall global

Global firewall settings.

```

config firewall global
    Description: Global firewall settings.
    set banned-ip-persistence [disabled|permanent-only|...]
end

```

config firewall global

Parameter	Description	Type	Size	Default
banned-ip-persistence	Persistency of banned IPs across power cycling.	option	-	disabled
	Option	Description		
	<i>disabled</i>	No entries are kept across power cycling.		
	<i>permanent-only</i>	Only permanent IP bans are kept across power cycling.		
	<i>all</i>	All IP bans are kept across power cycling.		

config firewall identity-based-route

Configure identity based routing.

```
config firewall identity-based-route
  Description: Configure identity based routing.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set device {string}
        set gateway {ipv4-address}
        set groups <name1>, <name2>, ...
      next
    end
  next
end
```

config firewall identity-based-route

Parameter	Description	Type	Size	Default
comments	Comments.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

config rule

Parameter	Description	Type	Size	Default
device	Outgoing interface for the rule.	string	Maximum length: 35	
gateway	IPv4 address of the gateway (Format: xxx.xxx.xxx.xxx , Default: 0.0.0.0).	ipv4-address	Not Specified	0.0.0.0
groups <name>	Select one or more group(s) from available groups that are allowed to use this route. Separate group names with a space. Group name.	string	Maximum length: 79	
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config firewall interface-policy

Configure IPv4 interface policies.

```
config firewall interface-policy
  Description: Configure IPv4 interface policies.
  edit <policyid>
    set application-list {string}
    set application-list-status [enable|disable]
    set av-profile {string}
    set av-profile-status [enable|disable]
    set casb-profile {string}
    set casb-profile-status [enable|disable]
    set comments {var-string}
    set dlp-profile {string}
    set dlp-profile-status [enable|disable]
    set dsri [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set emailfilter-profile {string}
    set emailfilter-profile-status [enable|disable]
    set interface {string}
    set ips-sensor {string}
    set ips-sensor-status [enable|disable]
    set logtraffic [all|utm|...]
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
    set uuid {uuid}
    set webfilter-profile {string}
    set webfilter-profile-status [enable|disable]
```

```
next
end
```

config firewall interface-policy

Parameter	Description	Type	Size	Default						
application-list	Application list name.	string	Maximum length: 47							
application-list-status	Enable/disable application control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable application control</td></tr><tr><td>disable</td><td>Disable application control</td></tr></table>	Option	Description	enable	Enable application control	disable	Disable application control			
Option	Description									
enable	Enable application control									
disable	Disable application control									
av-profile	Antivirus profile.	string	Maximum length: 47							
av-profile-status	Enable/disable antivirus.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable antivirus</td></tr><tr><td>disable</td><td>Disable antivirus</td></tr></table>	Option	Description	enable	Enable antivirus	disable	Disable antivirus			
Option	Description									
enable	Enable antivirus									
disable	Disable antivirus									
casb-profile	CASB profile.	string	Maximum length: 47							
casb-profile-status	Enable/disable CASB.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable CASB.</td></tr><tr><td>disable</td><td>Disable CASB.</td></tr></table>	Option	Description	enable	Enable CASB.	disable	Disable CASB.			
Option	Description									
enable	Enable CASB.									
disable	Disable CASB.									
comments	Comments.	var-string	Maximum length: 1023							
dlp-profile	DLP profile name.	string	Maximum length: 47							
dlp-profile-status	Enable/disable DLP.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dsri	Enable/disable DSRI.	option	-	disable
	Option Description			
	<i>enable</i>	Enable DSRI.		
	<i>disable</i>	Disable DSRI.		
dstaddr <name>	Address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79	
emailfilter-profile	Email filter profile.	string	Maximum length: 47	
emailfilter-profile-status	Enable/disable email filter.	option	-	disable
	Option Description			
	<i>enable</i>	Enable Email filter.		
	<i>disable</i>	Disable Email filter.		
interface	Monitored interface name from available interfaces.	string	Maximum length: 35	
ips-sensor	IPS sensor name.	string	Maximum length: 47	
ips-sensor-status	Enable/disable IPS.	option	-	disable
	Option Description			
	<i>enable</i>	Enable IPS.		
	<i>disable</i>	Disable IPS.		
logtraffic	Logging type to be used in this policy (Options: all utm disable, Default: utm).	option	-	utm
	Option Description			
	<i>all</i>	Log all sessions accepted or denied by this policy.		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>utm</i>	Log traffic that has a security profile applied to it.		
	<i>disable</i>	Disable all logging for this policy.		
policyid	Policy ID (0 - 4294967295).	integer	Minimum value: 0 0 Maximum value: 4294967295	
service <name>	Service object from available options. Service name.	string	Maximum length: 79	
srcaddr <name>	Address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79	
status	Enable/disable this policy.	option	-	enable
	Option Description			
	<i>enable</i>	Enable this policy.		
	<i>disable</i>	Disable this policy.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
webfilter-profile	Web filter profile.	string	Maximum length: 47	
webfilter-profile-status	Enable/disable web filtering.	option	-	disable
	Option Description			
	<i>enable</i>	Enable web filtering.		
	<i>disable</i>	Disable web filtering.		

config firewall interface-policy6

Configure IPv6 interface policies.

```
config firewall interface-policy6
    Description: Configure IPv6 interface policies.
    edit <policyid>
        set application-list {string}
```

```

set application-list-status [enable|disable]
set av-profile {string}
set av-profile-status [enable|disable]
set casb-profile {string}
set casb-profile-status [enable|disable]
set comments {var-string}
set dlp-profile {string}
set dlp-profile-status [enable|disable]
set dsri [enable|disable]
set dstaddr6 <name1>, <name2>, ...
set emailfilter-profile {string}
set emailfilter-profile-status [enable|disable]
set interface {string}
set ips-sensor {string}
set ips-sensor-status [enable|disable]
set logtraffic [all|utm|...]
set service6 <name1>, <name2>, ...
set srcaddr6 <name1>, <name2>, ...
set status [enable|disable]
set uuid {uuid}
set webfilter-profile {string}
set webfilter-profile-status [enable|disable]
next
end

```

config firewall interface-policy6

Parameter	Description	Type	Size	Default						
application-list	Application list name.	string	Maximum length: 47							
application-list-status	Enable/disable application control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable application control</td></tr><tr><td><i>disable</i></td><td>Disable application control</td></tr></table>	Option	Description	<i>enable</i>	Enable application control	<i>disable</i>	Disable application control			
Option	Description									
<i>enable</i>	Enable application control									
<i>disable</i>	Disable application control									
av-profile	Antivirus profile.	string	Maximum length: 47							
av-profile-status	Enable/disable antivirus.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable antivirus</td></tr><tr><td><i>disable</i></td><td>Disable antivirus</td></tr></table>	Option	Description	<i>enable</i>	Enable antivirus	<i>disable</i>	Disable antivirus			
Option	Description									
<i>enable</i>	Enable antivirus									
<i>disable</i>	Disable antivirus									

Parameter	Description	Type	Size	Default						
casb-profile	CASB profile.	string	Maximum length: 47							
casb-profile-status	Enable/disable CASB.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable CASB.</td></tr><tr><td>disable</td><td>Disable CASB.</td></tr></table>	Option	Description	enable	Enable CASB.	disable	Disable CASB.			
Option	Description									
enable	Enable CASB.									
disable	Disable CASB.									
comments	Comments.	var-string	Maximum length: 1023							
dlp-profile	DLP profile name.	string	Maximum length: 47							
dlp-profile-status	Enable/disable DLP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
dsri	Enable/disable DSRI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DSRI.</td></tr><tr><td>disable</td><td>Disable DSRI.</td></tr></table>	Option	Description	enable	Enable DSRI.	disable	Disable DSRI.			
Option	Description									
enable	Enable DSRI.									
disable	Disable DSRI.									
dstaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79							
emailfilter-profile	Email filter profile.	string	Maximum length: 47							
emailfilter-profile-status	Enable/disable email filter.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Email filter.</td></tr><tr><td>disable</td><td>Disable Email filter.</td></tr></table>	Option	Description	enable	Enable Email filter.	disable	Disable Email filter.			
Option	Description									
enable	Enable Email filter.									
disable	Disable Email filter.									

Parameter	Description	Type	Size	Default								
interface	Monitored interface name from available interfaces.	string	Maximum length: 35									
ips-sensor	IPS sensor name.	string	Maximum length: 47									
ips-sensor-status	Enable/disable IPS.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS.</td></tr><tr><td><i>disable</i></td><td>Disable IPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS.	<i>disable</i>	Disable IPS.					
Option	Description											
<i>enable</i>	Enable IPS.											
<i>disable</i>	Disable IPS.											
logtraffic	Logging type to be used in this policy (Options: all utm disable, Default: utm).	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
policyid	Policy ID (0 - 4294967295).	integer	Minimum value: 0 0 Maximum value: 4294967295									
service6 <name>	Service name. Service name.	string	Maximum length: 79									
srcaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79									
status	Enable/disable this policy.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.					
Option	Description											
<i>enable</i>	Enable this policy.											
<i>disable</i>	Disable this policy.											
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000								
webfilter-profile	Web filter profile.	string	Maximum length: 47									

Parameter	Description	Type	Size	Default
webfilter-profile-status	Enable/disable web filtering.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable web filtering.		
	<i>disable</i>	Disable web filtering.		

config firewall internet-service

Show Internet Service application. Read-only.

```

config firewall internet-service
  Description: Show Internet Service application. Read-only.
  edit <id>
    set database [isdb|irdb]
    set direction [src|dst|...]
    set extra-ip-range-number {integer}
    set extra-ip6-range-number {integer}
    set icon-id {integer}
    set ip-number {integer}
    set ip-range-number {integer}
    set ip6-range-number {integer}
    set name {string}
    set obsolete {integer}
    set singularity {integer}
  next
end

```

config firewall internet-service

Parameter	Description	Type	Size	Default
database	Database name this Internet Service belongs to. Read-only.	option	-	isdb
	Option	Description		
	<i>isdb</i>	Internet Service Database.		
	<i>irdb</i>	Internet RRR Database.		
direction	How this service may be used in a firewall policy (source, destination or both). Read-only.	option	-	both

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>src</i>	As source in the firewall policy.		
	<i>dst</i>	As destination in the firewall policy.		
	<i>both</i>	Both directions in the firewall policy.		
extra-ip-range-number	Extra number of IPv4 ranges. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
extra-ip6-range-number	Extra number of IPv6 ranges. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
icon-id	Icon ID of Internet Service. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
id	Internet Service ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
ip-number	Total number of IPv4 addresses. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
ip-range-number	Number of IPv4 ranges. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
ip6-range-number	Number of IPv6 ranges. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
name	Internet Service name. Read-only.	string	Maximum length: 63	
obsolete	Indicates whether the Internet Service can be used. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	
singularity	Singular level of the Internet Service. Read-only.	integer	Minimum value: 0 0 Maximum value: 65535	

config firewall internet-service-addition

Configure Internet Services Addition.

```
config firewall internet-service-addition
  Description: Configure Internet Services Addition.
  edit <id>
    set comment {var-string}
    config entry
      Description: Entries added to the Internet Service addition database.
      edit <id>
        set addr-mode [ipv4|ipv6]
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set end-port {integer}
            set start-port {integer}
          next
        end
        set protocol {integer}
      next
    end
  next
end
```

config firewall internet-service-addition

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
id	Internet Service ID in the Internet Service database.	integer	Minimum value: 0 Maximum value: 4294967295	

config entry

Parameter	Description	Type	Size	Default
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option	Description		
	ipv4	IPv4 mode.		
	ipv6	IPv6 mode.		

Parameter	Description	Type	Size	Default
id	Entry ID(1-255).	integer	Minimum value: 0 Maximum value: 255	0
protocol	Integer value for the protocol type as defined by IANA (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0

config port-range

Parameter	Description	Type	Size	Default
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1

config firewall internet-service-append

Configure additional port mappings for Internet Services.

```
config firewall internet-service-append
    Description: Configure additional port mappings for Internet Services.
    set addr-mode [ipv4|ipv6|...]
    set append-port {integer}
    set match-port {integer}
end
```

config firewall internet-service-append

Parameter	Description	Type	Size	Default
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ipv4</i>	IPv4 mode.		
	<i>ipv6</i>	IPv6 mode.		
	<i>both</i>	Both IPv4 and IPv6 mode.		
append-port	Appending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 0 Maximum value: 65535	0
match-port	Matching TCP/UDP/SCTP destination port (0 to 65535, 0 means any port).	integer	Minimum value: 0 Maximum value: 65535	0

config firewall internet-service-botnet

Show Internet Service botnet. Read-only.

```
config firewall internet-service-botnet
  Description: Show Internet Service botnet. Read-only.
  edit <id>
    set name {string}
  next
end
```

config firewall internet-service-botnet

Parameter	Description	Type	Size	Default
id	Internet Service Botnet ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service Botnet name.	string	Maximum length: 63	

config firewall internet-service-custom

Configure custom Internet Services.

```

config firewall internet-service-custom
    Description: Configure custom Internet Services.
    edit <name>
        set comment {var-string}
        config entry
            Description: Entries added to the Internet Service database and custom database.
            edit <id>
                set addr-mode [ipv4|ipv6]
                set dst <name1>, <name2>, ...
                set dst6 <name1>, <name2>, ...
                config port-range
                    Description: Port ranges in the custom entry.
                    edit <id>
                        set end-port {integer}
                        set start-port {integer}
                    next
                end
                set protocol {integer}
            next
        end
        set reputation {integer}
    next
end

```

config firewall internet-service-custom

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Internet Service name.	string	Maximum length: 63	
reputation	Reputation level of the custom Internet Service.	integer	Minimum value: 3 0 Maximum value: 4294967295	

config entry

Parameter	Description	Type	Size	Default						
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 mode.</td></tr><tr><td>ipv6</td><td>IPv6 mode.</td></tr></table>				Option	Description	ipv4	IPv4 mode.	ipv6	IPv6 mode.
	Option	Description								
	ipv4	IPv4 mode.								
ipv6	IPv6 mode.									

Parameter	Description	Type	Size	Default
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	
dst6 <name>	Destination address6 or address6 group name. Select the destination address6 or address group object from available options.	string	Maximum length: 79	
id	Entry ID(1-255).	integer	Minimum value: 0 Maximum value: 255	0
protocol	Integer value for the protocol type as defined by IANA (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0

config port-range

Parameter	Description	Type	Size	Default
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1

config firewall internet-service-custom-group

Configure custom Internet Service group.

```

config firewall internet-service-custom-group
    Description: Configure custom Internet Service group.
    edit <name>
        set comment {var-string}
        set member <name1>, <name2>, ...
    next
end

```

config firewall internet-service-custom-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
member <name>	Custom Internet Service group members. Group member name.	string	Maximum length: 79	
name	Custom Internet Service group name.	string	Maximum length: 63	

config firewall internet-service-definition

Configure Internet Service definition.

```
config firewall internet-service-definition
  Description: Configure Internet Service definition.
  edit <id>
    config entry
      Description: Protocol and port information in an Internet Service entry.
      edit <seq-num>
        set category-id {integer}
        set name {string}
        config port-range
          Description: Port ranges in the definition entry.
          edit <id>
            set end-port {integer}
            set start-port {integer}
          next
        end
        set protocol {integer}
      next
    end
  next
end
```

config firewall internet-service-definition

Parameter	Description	Type	Size	Default
id	Internet Service application list ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0

config entry

Parameter	Description	Type	Size	Default
category-id	Internet Service category ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service name. Read-only.	string	Maximum length: 63	
protocol	Integer value for the protocol type as defined by IANA (0 - 255). Read-only.	integer	Minimum value: 0 Maximum value: 255	0
seq-num	Entry sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0

config port-range

Parameter	Description	Type	Size	Default
end-port	Ending TCP/UDP/SCTP destination port (1 to 65535). Read-only.	integer	Minimum value: 1 Maximum value: 65535	65535
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Starting TCP/UDP/SCTP destination port (1 to 65535). Read-only.	integer	Minimum value: 1 Maximum value: 65535	1

config firewall internet-service-extension

Configure Internet Services Extension.

```
config firewall internet-service-extension
  Description: Configure Internet Services Extension.
  edit <id>
    set comment {var-string}
    config disable-entry
      Description: Disable entries in the Internet Service database.
      edit <id>
        set addr-mode [ipv4|ipv6]
```

```

    config ip-range
        Description: IPv4 ranges in the disable entry.
        edit <id>
            set end-ip {ipv4-address-any}
            set start-ip {ipv4-address-any}
        next
    end
    config ip6-range
        Description: IPv6 ranges in the disable entry.
        edit <id>
            set end-ip6 {ipv6-address}
            set start-ip6 {ipv6-address}
        next
    end
    config port-range
        Description: Port ranges in the disable entry.
        edit <id>
            set end-port {integer}
            set start-port {integer}
        next
    end
    set protocol {integer}
next
end
config entry
    Description: Entries added to the Internet Service extension database.
    edit <id>
        set addr-mode [ipv4|ipv6]
        set dst <name1>, <name2>, ...
        set dst6 <name1>, <name2>, ...
        config port-range
            Description: Port ranges in the custom entry.
            edit <id>
                set end-port {integer}
                set start-port {integer}
            next
        end
        set protocol {integer}
    next
end
next
end

```

config firewall internet-service-extension

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
id	Internet Service ID in the Internet Service database.	integer	Minimum value: 0 Maximum value: 4294967295	0

config disable-entry

Parameter	Description	Type	Size	Default						
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 mode.</td></tr><tr><td>ipv6</td><td>IPv6 mode.</td></tr></table>	Option	Description	ipv4	IPv4 mode.	ipv6	IPv6 mode.			
Option	Description									
ipv4	IPv4 mode.									
ipv6	IPv6 mode.									
id	Disable entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0						
protocol	Integer value for the protocol type as defined by IANA (0 - 255).	integer	Minimum value: 0 0 Maximum value: 255	0						

config ip-range

Parameter	Description	Type	Size	Default
end-ip	End IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
id	Disable entry range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0

config ip6-range

Parameter	Description	Type	Size	Default
end-ip6	End IPv6 address.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
id	Disable entry range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip6	Start IPv6 address.	ipv6-address	Not Specified	::

config port-range

Parameter	Description	Type	Size	Default
end-port	Ending TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Starting TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1

config entry

Parameter	Description	Type	Size	Default						
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 mode.</td></tr><tr><td>ipv6</td><td>IPv6 mode.</td></tr></table>	Option	Description	ipv4	IPv4 mode.	ipv6	IPv6 mode.			
Option	Description									
ipv4	IPv4 mode.									
ipv6	IPv6 mode.									
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79							
dst6 <name>	Destination address6 or address6 group name. Select the destination address6 or address group object from available options.	string	Maximum length: 79							
id	Entry ID(1-255).	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0

config port-range

Parameter	Description	Type	Size	Default
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1

config firewall internet-service-group

Configure group of Internet Service.

```
config firewall internet-service-group
  Description: Configure group of Internet Service.
  edit <name>
    set comment {var-string}
    set direction [source|destination|...]
    set member <name1>, <name2>, ...
  next
end
```

config firewall internet-service-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
direction	How this service may be used (source, destination or both).	option	-	both

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>source</i>	As source when applied.		
	<i>destination</i>	As destination when applied.		
	<i>both</i>	Both directions when applied.		
member <name>	Internet Service group member. Internet Service name.	string	Maximum length: 79	
name	Internet Service group name.	string	Maximum length: 63	

config firewall internet-service-ipbl-reason

IP block list reason. Read-only.

```
config firewall internet-service-ipbl-reason
  Description: IP block list reason. Read-only.
  edit <id>
    set name {string}
  next
end
```

config firewall internet-service-ipbl-reason

Parameter	Description	Type	Size	Default
id	IP block list reason ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	IP block list reason name.	string	Maximum length: 63	

config firewall internet-service-ipbl-vendor

IP block list vendor. Read-only.

```
config firewall internet-service-ipbl-vendor
  Description: IP block list vendor. Read-only.
  edit <id>
    set name {string}
```

```
next
end
```

config firewall internet-service-ipbl-vendor

Parameter	Description	Type	Size	Default
id	IP block list vendor ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	IP block list vendor name.	string	Maximum length: 63	

config firewall internet-service-list

Internet Service list. Read-only.

```
config firewall internet-service-list
  Description: Internet Service list. Read-only.
  edit <id>
    set name {string}
  next
end
```

config firewall internet-service-list

Parameter	Description	Type	Size	Default
id	Internet Service category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service category name.	string	Maximum length: 63	

config firewall internet-service-name

Define internet service names.

```
config firewall internet-service-name
  Description: Define internet service names.
```

```

edit <name>
    set city-id {integer}
    set country-id {integer}
    set internet-service-id {integer}
    set region-id {integer}
    set type [default|location]
next
end

```

config firewall internet-service-name

Parameter	Description	Type	Size	Default
city-id	City ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
country-id	Country or Area ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
internet-service-id	Internet Service ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
name	Internet Service name.	string	Maximum length: 63	
region-id	Region ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
type	Internet Service name type.	option	-	default
	Option	Description		
	default	Automatically generated Internet Service.		
	location	Geography location based Internet Service.		

config firewall internet-service-owner

Internet Service owner. Read-only.

```

config firewall internet-service-owner
    Description: Internet Service owner. Read-only.

```

```
edit <id>
    set name {string}
next
end
```

config firewall internet-service-owner

Parameter	Description	Type	Size	Default
id	Internet Service owner ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service owner name.	string	Maximum length: 63	

config firewall internet-service-reputation

Show Internet Service reputation. Read-only.

```
config firewall internet-service-reputation
    Description: Show Internet Service reputation. Read-only.
    edit <id>
        set description {string}
    next
end
```

config firewall internet-service-reputation

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
id	Internet Service Reputation ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config firewall internet-service-sld

Internet Service Second Level Domain. Read-only.

```

config firewall internet-service-sld
    Description: Internet Service Second Level Domain. Read-only.
    edit <id>
        set name {string}
    next
end

```

config firewall internet-service-sld

Parameter	Description	Type	Size	Default
id	Second Level Domain ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
name	Second Level Domain name.	string	Maximum length: 63	

config firewall internet-service-subapp

Show Internet Service sub app ID. Read-only.

```

config firewall internet-service-subapp
    Description: Show Internet Service sub app ID. Read-only.
    edit <id>
        set sub-app <id1>, <id2>, ...
    next
end

```

config firewall internet-service-subapp

Parameter	Description	Type	Size	Default
id	Internet Service main ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
sub-app <id>	Subapp number list. Subapp ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config firewall ipmacbinding setting

Configure IP to MAC binding settings.

```
config firewall ipmacbinding setting
  Description: Configure IP to MAC binding settings.
  set bindthroughfw [enable|disable]
  set bindtofw [enable|disable]
  set undefinedhost [allow|block]
end
```

config firewall ipmacbinding setting

Parameter	Description	Type	Size	Default						
bindthroughfw	Enable/disable use of IP/MAC binding to filter packets that would normally go through the firewall.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP/MAC binding for packets that would normally go through the firewall.</td></tr><tr><td><i>disable</i></td><td>Disable IP/MAC binding for packets that would normally go through the firewall.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP/MAC binding for packets that would normally go through the firewall.	<i>disable</i>	Disable IP/MAC binding for packets that would normally go through the firewall.			
Option	Description									
<i>enable</i>	Enable IP/MAC binding for packets that would normally go through the firewall.									
<i>disable</i>	Disable IP/MAC binding for packets that would normally go through the firewall.									
bindtofw	Enable/disable use of IP/MAC binding to filter packets that would normally go to the firewall.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP/MAC binding for packets that would normally go to the firewall.</td></tr><tr><td><i>disable</i></td><td>Disable IP/MAC binding for packets that would normally go to the firewall.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP/MAC binding for packets that would normally go to the firewall.	<i>disable</i>	Disable IP/MAC binding for packets that would normally go to the firewall.			
Option	Description									
<i>enable</i>	Enable IP/MAC binding for packets that would normally go to the firewall.									
<i>disable</i>	Disable IP/MAC binding for packets that would normally go to the firewall.									
undefinedhost	Select action to take on packets with IP/MAC addresses not in the binding list (default = block).	option	-	block						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow packets from MAC addresses not in the IP/MAC list.</td></tr><tr><td><i>block</i></td><td>Block packets from MAC addresses not in the IP/MAC list.</td></tr></table>	Option	Description	<i>allow</i>	Allow packets from MAC addresses not in the IP/MAC list.	<i>block</i>	Block packets from MAC addresses not in the IP/MAC list.			
Option	Description									
<i>allow</i>	Allow packets from MAC addresses not in the IP/MAC list.									
<i>block</i>	Block packets from MAC addresses not in the IP/MAC list.									

config firewall ipmacbinding table

Configure IP to MAC address pairs in the IP/MAC binding table.

```

config firewall ipmacbinding table
    Description: Configure IP to MAC address pairs in the IP/MAC binding table.
    edit <seq-num>
        set ip {ipv4-address}
        set mac {mac-address}
        set name {string}
        set status [enable|disable]
    next
end

```

config firewall ipmacbinding table

Parameter	Description	Type	Size	Default
ip	IPv4 address portion of the pair (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
mac	MAC address portion of the pair (format = xx:xx:xx:xx:xx:xx in hexadecimal).	mac-address	Not Specified	00:00:00:00:00:00
name	Name of the pair (optional, default = no name).	string	Maximum length: 35	noname
seq-num	Entry number.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable this IP-mac binding pair.	option	-	disable

Option	Description
<i>enable</i>	Enable this IP-mac binding pair.
<i>disable</i>	Disable this IP-mac binding pair.

config firewall ippool

Configure IPv4 IP pools.

```

config firewall ippool
    Description: Configure IPv4 IP pools.
    edit <name>
        set add-nat64-route [disable|enable]
        set arp-intf {string}
        set arp-reply [disable|enable]
        set associated-interface {string}
        set block-size {integer}
    end
end

```



```

set cgn-block-size {integer}
set cgn-client-endip {var-string}
set cgn-client-ipv6shift {integer}
set cgn-client-startip {var-string}
set cgn-fixedalloc [disable|enable]
set cgn-overload [disable|enable]
set cgn-port-end {integer}
set cgn-port-start {integer}
set cgn-spa [disable|enable]
set client-prefix-length {integer}
set comments {var-string}
set endip {ipv4-address-any}
set endport {integer}
set exclude-ip <ip1>, <ip2>, ...
set icmp-session-quota {integer}
set nat64 [disable|enable]
set num-blocks-per-user {integer}
set pba-interim-log {integer}
set pba-timeout {integer}
set permit-any-host [disable|enable]
set port-per-user {integer}
set privileged-port-use-pba [disable|enable]
set source-endip {ipv4-address-any}
set source-prefix6 {ipv6-network}
set source-startip {ipv4-address-any}
set startip {ipv4-address-any}
set startport {integer}
set subnet-broadcast-in-ippool {option}
set tcp-session-quota {integer}
set type [overload|one-to-one|...]
set udp-session-quota {integer}
set utilization-alarm-clear {integer}
set utilization-alarm-raise {integer}
next
end

```

config firewall ippool

Parameter	Description	Type	Size	Default						
add-nat64-route	Enable/disable adding NAT64 route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable adding NAT64 route.</td></tr><tr><td><i>enable</i></td><td>Enable adding NAT64 route.</td></tr></table>	Option	Description	<i>disable</i>	Disable adding NAT64 route.	<i>enable</i>	Enable adding NAT64 route.			
Option	Description									
<i>disable</i>	Disable adding NAT64 route.									
<i>enable</i>	Enable adding NAT64 route.									

Parameter	Description	Type	Size	Default						
arp-intf	Select an interface from available options that will reply to ARP requests. (If blank, any is selected).	string	Maximum length: 15							
arp-reply	Enable/disable replying to ARP requests when an IP Pool is added to a policy (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable ARP reply.</td></tr><tr><td>enable</td><td>Enable ARP reply.</td></tr></table>	Option	Description	disable	Disable ARP reply.	enable	Enable ARP reply.			
Option	Description									
disable	Disable ARP reply.									
enable	Enable ARP reply.									
associated-interface	Associated interface name.	string	Maximum length: 15							
block-size	Number of addresses in a block (64 - 4096, default = 128).	integer	Minimum value: 64 Maximum value: 4096	128						
cgn-block-size *	Number of ports in a block(64 to 4096 in unit of 64, default = 128).	integer	Minimum value: 64 Maximum value: 4096	128						
cgn-client-endip *	Final client IPv4 address (inclusive) (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	var-string	Maximum length: 255							
cgn-client-ipv6shift *	IPv6 shift for fixed-allocation.(default 0)	integer	Minimum value: 0 Maximum value: 127	0						
cgn-client-startip *	First client IPv4 address (inclusive) (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	var-string	Maximum length: 255							
cgn-fixedalloc *	Enable/disable fixed-allocation mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable fixed-allocation mode.</td></tr><tr><td>enable</td><td>Enable fixed-allocation mode.</td></tr></table>	Option	Description	disable	Disable fixed-allocation mode.	enable	Enable fixed-allocation mode.			
Option	Description									
disable	Disable fixed-allocation mode.									
enable	Enable fixed-allocation mode.									
cgn-overload *	Enable/disable overload mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable overload mode.</td></tr><tr><td>enable</td><td>Enable overload mode.</td></tr></table>	Option	Description	disable	Disable overload mode.	enable	Enable overload mode.			
Option	Description									
disable	Disable overload mode.									
enable	Enable overload mode.									

Parameter	Description	Type	Size	Default
cgn-port-end *	Ending public port can be allocated.	integer	Minimum value: 1024 Maximum value: 65535	65530
cgn-port-start *	Starting public port can be allocated.	integer	Minimum value: 1024 Maximum value: 65535	5117
cgn-spa *	Enable/disable single port allocation mode.	option	-	disable
	Option	Description		
	disable	Disable SPA mode.		
	enable	Enable SPA mode.		
client-prefix-length	Subnet length of a single deterministic NAT64 client (1 - 128, default = 64).	integer	Minimum value: 1 Maximum value: 128	64
comments	Comment.	var-string	Maximum length: 255	
endip	Final IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
endport	Final port number (inclusive) in the range for the address pool (1024 - 65535, Default: 65533).	integer	Minimum value: 1024 Maximum value: 65535	65533
exclude-ip <ip> *	Exclude IPs x.x.x.x. Exclude IPs (xxx.xxx.xxx.xxx)	string	Maximum length: 79	
icmp-session-quota	Maximum number of concurrent ICMP sessions allowed per client (0 - 2097000, default = 0 which means no limit).	integer	Minimum value: 0 Maximum value: 2097000	0
name	IP pool name.	string	Maximum length: 79	
nat64	Enable/disable NAT64.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable DNAT64.		
	<i>enable</i>	Enable DNAT64.		
num-blocks-per-user	Number of addresses blocks that can be used by a user (1 to 128, default = 8).	integer	Minimum value: 1 Maximum value: 128	8
pba-interim-log	Port block allocation interim logging interval (600 - 86400 seconds, default = 0 which disables interim logging).	integer	Minimum value: 600 Maximum value: 86400	0
pba-timeout	Port block allocation timeout (seconds).	integer	Minimum value: 3 Maximum value: 86400	30
permit-any-host	Enable/disable full cone NAT.	option	-	disable
	Option Description			
	<i>disable</i>	Disable full cone NAT.		
	<i>enable</i>	Enable full cone NAT.		
port-per-user	Number of port for each user (32 - 60416, default = 0, which is auto).	integer	Minimum value: 32 Maximum value: 60417	0
privileged-port-use-pba	Enable/disable selection of the external port from the port block allocation for NAT'ing privileged ports (default = disable).	option	-	disable
	Option Description			
	<i>disable</i>	Select new nat port for privileged source ports from privileged range 512-1023.		
	<i>enable</i>	Select new nat port for privileged source ports from client's port block		

Parameter	Description	Type	Size	Default										
source-endip	Final IPv4 address (inclusive) in the range of the source addresses to be translated (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0										
source-prefix6	Source IPv6 network to be translated (format = xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx, default = ::/0).	ipv6-network	Not Specified	::/0										
source-startip	First IPv4 address (inclusive) in the range of the source addresses to be translated (format = xxx.xxx.xxx.xxx, default = 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0										
startip	First IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0										
startport	First port number (inclusive) in the range for the address pool (1024 - 65535, Default: 5117).	integer	Minimum value: 1024 Maximum value: 65535	5117										
subnet-broadcast-in-ippool	Enable/disable inclusion of the subnetwork address and broadcast IP address in the NAT64 IP pool.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not include the subnetwork address and broadcast IP address in the NAT64 IP pool.</td></tr></table>				Option	Description	disable	Do not include the subnetwork address and broadcast IP address in the NAT64 IP pool.						
Option	Description													
disable	Do not include the subnetwork address and broadcast IP address in the NAT64 IP pool.													
tcp-session-quota	Maximum number of concurrent TCP sessions allowed per client (0 - 2097000, default = 0 which means no limit).	integer	Minimum value: 0 Maximum value: 2097000	0										
type	IP pool type: overload, one-to-one, fixed-port-range, port-block-allocation, cgn-resource-allocation (hyperscale vdom only)	option	-	overload										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>overload</td><td>IP addresses in the IP pool can be shared by clients.</td></tr><tr><td>one-to-one</td><td>One to one mapping.</td></tr><tr><td>fixed-port-range</td><td>Fixed port range.</td></tr><tr><td>port-block-allocation</td><td>Port block allocation.</td></tr></table>				Option	Description	overload	IP addresses in the IP pool can be shared by clients.	one-to-one	One to one mapping.	fixed-port-range	Fixed port range.	port-block-allocation	Port block allocation.
Option	Description													
overload	IP addresses in the IP pool can be shared by clients.													
one-to-one	One to one mapping.													
fixed-port-range	Fixed port range.													
port-block-allocation	Port block allocation.													

Parameter	Description	Type	Size	Default
udp-session-quota	Maximum number of concurrent UDP sessions allowed per client (0 - 2097000, default = 0 which means no limit).	integer	Minimum value: 0 Maximum value: 2097000	0
utilization-alarm-clear *	Pool utilization alarm clear threshold (40-100).	integer	Minimum value: 40 Maximum value: 100	80
utilization-alarm-raise *	Pool utilization alarm raise threshold (50-100).	integer	Minimum value: 50 Maximum value: 100	100

* This parameter may not exist in some models.

config firewall ippool6

Configure IPv6 IP pools.

```
config firewall ippool6
  Description: Configure IPv6 IP pools.
  edit <name>
    set add-nat46-route [disable|enable]
    set comments {var-string}
    set endip {ipv6-address}
    set external-prefix {ipv6-network}
    set internal-prefix {ipv6-network}
    set nat46 [disable|enable]
    set startip {ipv6-address}
    set type [overload|nptv6]
  next
end
```

config firewall ippool6

Parameter	Description	Type	Size	Default
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable adding NAT46 route.</td></tr><tr><td><i>enable</i></td><td>Enable adding NAT46 route.</td></tr></table>	Option	Description	<i>disable</i>	Disable adding NAT46 route.	<i>enable</i>	Enable adding NAT46 route.			
	Option	Description								
	<i>disable</i>	Disable adding NAT46 route.								
<i>enable</i>	Enable adding NAT46 route.									
comments	Comment.	var-string	Maximum length: 255							
endip	Final IPv6 address (inclusive) in the range for the address pool (format = xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, default = ::).	ipv6-address	Not Specified	::						
external-prefix	External NPTv6 prefix length (32 - 64).	ipv6-network	Not Specified	::/0						
internal-prefix	Internal NPTv6 prefix length (32 - 64).	ipv6-network	Not Specified	::/0						
name	IPv6 IP pool name.	string	Maximum length: 79							
nat46	Enable/disable NAT46.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NAT46.</td></tr><tr><td><i>enable</i></td><td>Enable NAT46.</td></tr></table>	Option	Description	<i>disable</i>	Disable NAT46.	<i>enable</i>	Enable NAT46.			
	Option	Description								
	<i>disable</i>	Disable NAT46.								
<i>enable</i>	Enable NAT46.									
startip	First IPv6 address (inclusive) in the range for the address pool (format = xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, default = ::).	ipv6-address	Not Specified	::						
type	Configure IPv6 pool type (overload or NPTv6).	option	-	overload						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>overload</i></td><td>IPv6 addresses in the IP pool can be shared by clients.</td></tr><tr><td><i>nptv6</i></td><td>NPTv6 one to one mapping.</td></tr></table>	Option	Description	<i>overload</i>	IPv6 addresses in the IP pool can be shared by clients.	<i>nptv6</i>	NPTv6 one to one mapping.			
	Option	Description								
	<i>overload</i>	IPv6 addresses in the IP pool can be shared by clients.								
<i>nptv6</i>	NPTv6 one to one mapping.									

config firewall ipv6-eh-filter

Configure IPv6 extension header filter.

```
config firewall ipv6-eh-filter
  Description: Configure IPv6 extension header filter.
  set auth [enable|disable]
```

```

set dest-opt [enable|disable]
set fragment [enable|disable]
set hdopt-type {integer}
set hop-opt [enable|disable]
set no-next [enable|disable]
set routing [enable|disable]
set routing-type {integer}
end

```

config firewall ipv6-e-h-filter

Parameter	Description	Type	Size	Default						
auth	Enable/disable blocking packets with the Authentication header (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Block packets with the Authentication header.</td></tr><tr><td><i>disable</i></td><td>Allow packets with the Authentication header.</td></tr></table>	Option	Description	<i>enable</i>	Block packets with the Authentication header.	<i>disable</i>	Allow packets with the Authentication header.			
Option	Description									
<i>enable</i>	Block packets with the Authentication header.									
<i>disable</i>	Allow packets with the Authentication header.									
dest-opt	Enable/disable blocking packets with Destination Options headers (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable blocking packets with Destination Options headers.</td></tr><tr><td><i>disable</i></td><td>Disable blocking packets with Destination Options headers.</td></tr></table>	Option	Description	<i>enable</i>	Enable blocking packets with Destination Options headers.	<i>disable</i>	Disable blocking packets with Destination Options headers.			
Option	Description									
<i>enable</i>	Enable blocking packets with Destination Options headers.									
<i>disable</i>	Disable blocking packets with Destination Options headers.									
fragment	Enable/disable blocking packets with the Fragment header (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Block packets with the Fragment header.</td></tr><tr><td><i>disable</i></td><td>Allow packets with the Fragment header.</td></tr></table>	Option	Description	<i>enable</i>	Block packets with the Fragment header.	<i>disable</i>	Allow packets with the Fragment header.			
Option	Description									
<i>enable</i>	Block packets with the Fragment header.									
<i>disable</i>	Allow packets with the Fragment header.									
hdopt-type	Block specific Hop-by-Hop and/or Destination Option types (max. 7 types, each between 0 and 255).	integer	Minimum value: 0 Maximum value: 255							
hop-opt	Enable/disable blocking packets with the Hop-by-Hop Options header (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable blocking packets with the Hop-by-Hop Options header.</td></tr><tr><td><i>disable</i></td><td>Disable blocking packets with the Hop-by-Hop Options header.</td></tr></table>	Option	Description	<i>enable</i>	Enable blocking packets with the Hop-by-Hop Options header.	<i>disable</i>	Disable blocking packets with the Hop-by-Hop Options header.			
Option	Description									
<i>enable</i>	Enable blocking packets with the Hop-by-Hop Options header.									
<i>disable</i>	Disable blocking packets with the Hop-by-Hop Options header.									

Parameter	Description	Type	Size	Default
no-next	Enable/disable blocking packets with the No Next header (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Block packets with the No Next header.		
	<i>disable</i>	Allow packets with the No Next header.		
routing	Enable/disable blocking packets with Routing headers (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Block packets with Routing headers.		
	<i>disable</i>	Allow packets with Routing headers.		
routing-type	Block specific Routing header types (max. 7 types, each between 0 and 255, default = 0).	integer	Minimum value: 0 Maximum value: 255	0

config firewall ip-translation

Configure firewall IP-translation.

```
config firewall ip-translation
  Description: Configure firewall IP-translation.
  edit <transid>
    set endip {ipv4-address-any}
    set map-startip {ipv4-address-any}
    set startip {ipv4-address-any}
    set type {option}
  next
end
```

config firewall ip-translation

Parameter	Description	Type	Size	Default
endip	Final IPv4 address (inclusive) in the range of the addresses to be translated (format xxx.xxx.xxx.xxx, default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
map-startip	Address to be used as the starting point for translation in the range (format xxx.xxx.xxx.xxx, default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
startip	First IPv4 address (inclusive) in the range of the addresses to be translated (format xxx.xxx.xxx.xxx, default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
transid	IP translation ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	IP translation type (option: SCTP).	option	-	SCTP
		Option	Description	
		SCTP	SCTP	

config firewall ldb-monitor

Configure server load balancing health monitors.

```
config firewall ldb-monitor
  Description: Configure server load balancing health monitors.
  edit <name>
    set dns-match-ip {ipv4-address}
    set dns-protocol [udp|tcp]
    set dns-request-domain {string}
    set http-get {string}
    set http-match {string}
    set http-max-redirects {integer}
    set interval {integer}
    set port {integer}
    set retry {integer}
    set src-ip {ipv4-address}
    set timeout {integer}
    set type [ping|tcp|...]
  next
end
```

config firewall ldb-monitor

Parameter	Description	Type	Size	Default
dns-match-ip	Response IP expected from DNS server.	ipv4-address	Not Specified	0.0.0.0
dns-protocol	Select the protocol used by the DNS health check monitor to check the health of the server (UDP TCP).	option	-	udp
	Option	Description		
	udp	UDP.		
	tcp	TCP.		
dns-request-domain	Fully qualified domain name to resolve for the DNS probe.	string	Maximum length: 255	
http-get	Request URI used to send a GET request to check the health of an HTTP server. Optionally provide a hostname before the first '/' and it will be used as the HTTP Host Header.	string	Maximum length: 255	
http-match	String to match the value expected in response to an HTTP-GET request.	string	Maximum length: 255	
http-max-redirects	The maximum number of HTTP redirects to be allowed (0 - 5, default = 0).	integer	Minimum value: 0 Maximum value: 5	0
interval	Time between health checks (5 - 65535 sec, default = 10).	integer	Minimum value: 5 Maximum value: 65535	10
name	Monitor name.	string	Maximum length: 35	
port	Service port used to perform the health check. If 0, health check monitor inherits port configured for the server (0 - 65535, default = 0).	integer	Minimum value: 0 Maximum value: 65535	0
retry	Number health check attempts before the server is considered down (1 - 255, default = 3).	integer	Minimum value: 1 Maximum value: 255	3

Parameter	Description	Type	Size	Default												
src-ip	Source IP for Idb-monitor.	ipv4-address	Not Specified	0.0.0.0												
timeout	Time to wait to receive response to a health check from a server. Reaching the timeout means the health check failed (1 - 255 sec, default = 2).	integer	Minimum value: 1 Maximum value: 255	2												
type	Select the Monitor type used by the health check monitor to check the health of the server (PING TCP HTTP HTTPS DNS).	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING health monitor.</td></tr><tr><td>tcp</td><td>TCP-connect health monitor.</td></tr><tr><td>http</td><td>HTTP-GET health monitor.</td></tr><tr><td>https</td><td>HTTP-GET health monitor with SSL.</td></tr><tr><td>dns</td><td>DNS health monitor.</td></tr></table>				Option	Description	ping	PING health monitor.	tcp	TCP-connect health monitor.	http	HTTP-GET health monitor.	https	HTTP-GET health monitor with SSL.	dns	DNS health monitor.
Option	Description															
ping	PING health monitor.															
tcp	TCP-connect health monitor.															
http	HTTP-GET health monitor.															
https	HTTP-GET health monitor with SSL.															
dns	DNS health monitor.															

config firewall local-in-policy

Configure user defined IPv4 local-in policies.

```
config firewall local-in-policy
  Description: Configure user defined IPv4 local-in policies.
  edit <policyid>
    set action [accept|deny]
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set ha-mgmt-intf-only [enable|disable]
    set internet-service-src [enable|disable]
    set internet-service-src-custom <name1>, <name2>, ...
    set internet-service-src-custom-group <name1>, <name2>, ...
    set internet-service-src-group <name1>, <name2>, ...
    set internet-service-src-name <name1>, <name2>, ...
    set internet-service-src-negate [enable|disable]
    set intf <name1>, <name2>, ...
    set logtraffic [enable|disable]
    set schedule {string}
    set service <name1>, <name2>, ...
    set service-negate [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set srcaddr-negate [enable|disable]
    set status [enable|disable]
```

```

        set uuid {uuid}
        set virtual-patch [enable|disable]
    next
end

```

config firewall local-in-policy

Parameter	Description	Type	Size	Default
action	Action performed on traffic matching the policy (default = deny).	option	-	deny
	Option Description			
	accept	Allow traffic matching this policy.		
	deny	Deny or block traffic matching this policy.		
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79	
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable
	Option Description			
	enable	Enable destination address negate.		
	disable	Disable destination address negate.		
ha-mgmt-intf-only	Enable/disable dedicating the HA management interface only for local-in policy.	option	-	disable
	Option Description			
	enable	Enable dedicating HA management interface only for local-in policy.		
	disable	Disable dedicating HA management interface only for local-in policy.		
internet-service-src	Enable/disable use of Internet Services in source for this local-in policy. If enabled, source address is not used.	option	-	disable
	Option Description			
	enable	Enable use of Internet Services source in local-in policy.		
	disable	Disable use of Internet Services source in local-in policy.		

Parameter	Description	Type	Size	Default						
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated Internet Service source match.</td></tr><tr><td>disable</td><td>Disable negated Internet Service source match.</td></tr></table>				Option	Description	enable	Enable negated Internet Service source match.	disable	Disable negated Internet Service source match.
Option	Description									
enable	Enable negated Internet Service source match.									
disable	Disable negated Internet Service source match.									
intf <name>	Incoming interface name from available options. Address name.	string	Maximum length: 79							
logtraffic	Enable/disable local-in traffic logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable local-in traffic logging.</td></tr><tr><td>disable</td><td>Disable local-in traffic logging.</td></tr></table>				Option	Description	enable	Enable local-in traffic logging.	disable	Disable local-in traffic logging.
Option	Description									
enable	Enable local-in traffic logging.									
disable	Disable local-in traffic logging.									
policyid	User defined local in policy ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
schedule	Schedule object from available options.	string	Maximum length: 35							
service <name>	Service object from available options. Service name.	string	Maximum length: 79							
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable negated service match.		
	<i>disable</i>	Disable negated service match.		
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79	
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable
	Option Description			
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable source address negate.		
status	Enable/disable this local-in policy.	option	-	enable
	Option Description			
	<i>enable</i>	Enable this local-in policy.		
	<i>disable</i>	Disable this local-in policy.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
virtual-patch	Enable/disable virtual patching.	option	-	disable
	Option Description			
	<i>enable</i>	Enable virtual patching.		
	<i>disable</i>	Disable virtual patching.		

config firewall local-in-policy6

Configure user defined IPv6 local-in policies.

```
config firewall local-in-policy6
  Description: Configure user defined IPv6 local-in policies.
  edit <policyid>
    set action [accept|deny]
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set internet-service6-src [enable|disable]
```

```

set internet-service6-src-custom <name1>, <name2>, ...
set internet-service6-src-custom-group <name1>, <name2>, ...
set internet-service6-src-group <name1>, <name2>, ...
set internet-service6-src-name <name1>, <name2>, ...
set internet-service6-src-negate [enable|disable]
set intf <name1>, <name2>, ...
set logtraffic [enable|disable]
set schedule {string}
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set status [enable|disable]
set uuid {uuid}
set virtual-patch [enable|disable]
next
end

```

config firewall local-in-policy6

Parameter	Description	Type	Size	Default						
action	Action performed on traffic matching the policy (default = deny).	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>accept</td><td>Allow local-in traffic matching this policy.</td></tr><tr><td>deny</td><td>Deny or block local-in traffic matching this policy.</td></tr></table>	Option	Description	accept	Allow local-in traffic matching this policy.	deny	Deny or block local-in traffic matching this policy.			
Option	Description									
accept	Allow local-in traffic matching this policy.									
deny	Deny or block local-in traffic matching this policy.									
comments	Comment.	var-string	Maximum length: 1023							
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79							
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable destination address negate.</td></tr><tr><td>disable</td><td>Disable destination address negate.</td></tr></table>	Option	Description	enable	Enable destination address negate.	disable	Disable destination address negate.			
Option	Description									
enable	Enable destination address negate.									
disable	Disable destination address negate.									
internet-service6-src	Enable/disable use of IPv6 Internet Services in source for this local-in policy.If enabled, source address is not used.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable use of IPv6 Internet Services source in local-in policy.		
	<i>disable</i>	Disable use of IPv6 Internet Services source in local-in policy.		
internet-service6-src-custom <name>	Custom IPv6 Internet Service source name. Custom Internet Service name.	string	Maximum length: 79	
internet-service6-src-custom-group <name>	Custom Internet Service6 source group name. Custom Internet Service6 group name.	string	Maximum length: 79	
internet-service6-src-group <name>	Internet Service6 source group name. Internet Service group name.	string	Maximum length: 79	
internet-service6-src-name <name>	IPv6 Internet Service source name. Internet Service name.	string	Maximum length: 79	
internet-service6-src-negate	When enabled internet-service6-src specifies what the service must NOT be.	option	-	disable
	Option Description			
	<i>enable</i>	Enable negated IPv6 Internet Service source match.		
	<i>disable</i>	Disable negated IPv6 Internet Service source match.		
intf <name>	Incoming interface name from available options. Address name.	string	Maximum length: 79	
logtraffic	Enable/disable local-in traffic logging.	option	-	disable
	Option Description			
	<i>enable</i>	Enable local-in traffic logging.		
	<i>disable</i>	Disable local-in traffic logging.		
policyid	User defined local in policy ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default						
schedule	Schedule object from available options.	string	Maximum length: 35							
service <name>	Service object from available options. Separate names with a space. Service name.	string	Maximum length: 79							
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated service match.</td></tr><tr><td>disable</td><td>Disable negated service match.</td></tr></table>	Option	Description	enable	Enable negated service match.	disable	Disable negated service match.			
Option	Description									
enable	Enable negated service match.									
disable	Disable negated service match.									
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source address negate.</td></tr><tr><td>disable</td><td>Disable source address negate.</td></tr></table>	Option	Description	enable	Enable source address negate.	disable	Disable source address negate.			
Option	Description									
enable	Enable source address negate.									
disable	Disable source address negate.									
status	Enable/disable this local-in policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this local-in policy.</td></tr><tr><td>disable</td><td>Disable this local-in policy.</td></tr></table>	Option	Description	enable	Enable this local-in policy.	disable	Disable this local-in policy.			
Option	Description									
enable	Enable this local-in policy.									
disable	Disable this local-in policy.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
virtual-patch	Enable/disable the virtual patching feature.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									

config firewall multicast-address

Configure multicast addresses.

```
config firewall multicast-address
  Description: Configure multicast addresses.
  edit <name>
    set associated-interface {string}
    set color {integer}
    set comment {var-string}
    set end-ip {ipv4-address-any}
    set start-ip {ipv4-address-any}
    set subnet {ipv4-classnet-any}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set type [multicastrange|broadcastmask]
  next
end
```

config firewall multicast-address

Parameter	Description	Type	Size	Default
associated-interface	Interface associated with the address object. When setting up a policy, only addresses associated with this interface are available.	string	Maximum length: 35	
color	Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1).	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
end-ip	Final IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
name	Multicast address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
start-ip	First IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0						
subnet	Broadcast address and subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0						
type	Type of address object: multicast IP address range or broadcast IP/mask to be treated as a multicast address.	option	-	multicastrange						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>multicastrange</i></td><td>Multicast range.</td></tr><tr><td><i>broadcastmask</i></td><td>Broadcast IP/mask.</td></tr></table>				Option	Description	<i>multicastrange</i>	Multicast range.	<i>broadcastmask</i>	Broadcast IP/mask.
Option	Description									
<i>multicastrange</i>	Multicast range.									
<i>broadcastmask</i>	Broadcast IP/mask.									

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall multicast-address6

Configure IPv6 multicast address.

```

config firewall multicast-address6
  Description: Configure IPv6 multicast address.
  edit <name>
    set color {integer}
    set comment {var-string}
    set ip6 {ipv6-network}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
  end

```

```
next
end
```

config firewall multicast-address6

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified	::/0
name	IPv6 multicast address name.	string	Maximum length: 79	

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall multicast-policy

Configure multicast NAT policies.

```
config firewall multicast-policy
  Description: Configure multicast NAT policies.
  edit <id>
    set action [accept|deny]
    set auto-asic-offload [enable|disable]
    set comments {var-string}
    set dnat {ipv4-address-any}
    set dstaddr <name1>, <name2>, ...
    set dstintf {string}
    set end-port {integer}
    set ips-sensor {string}
```

```

set logtraffic [all|utm|...]
set name {string}
set protocol {integer}
set snat [enable|disable]
set snat-ip {ipv4-address}
set srcaddr <name1>, <name2>, ...
set srcintf {string}
set start-port {integer}
set status [enable|disable]
set traffic-shaper {string}
set utm-status [enable|disable]
set uuid {uuid}

next
end

```

config firewall multicast-policy

Parameter	Description	Type	Size	Default						
action	Accept or deny traffic matching the policy.	option	-	accept						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept traffic matching the policy.</td></tr><tr><td><i>deny</i></td><td>Deny or block traffic matching the policy.</td></tr></table>	Option	Description	<i>accept</i>	Accept traffic matching the policy.	<i>deny</i>	Deny or block traffic matching the policy.			
Option	Description									
<i>accept</i>	Accept traffic matching the policy.									
<i>deny</i>	Deny or block traffic matching the policy.									
auto-asic-offload	Enable/disable offloading policy traffic for hardware acceleration.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable hardware acceleration offloading.</td></tr><tr><td><i>disable</i></td><td>Disable offloading for hardware acceleration.</td></tr></table>	Option	Description	<i>enable</i>	Enable hardware acceleration offloading.	<i>disable</i>	Disable offloading for hardware acceleration.			
Option	Description									
<i>enable</i>	Enable hardware acceleration offloading.									
<i>disable</i>	Disable offloading for hardware acceleration.									
comments	Comment.	var-string	Maximum length: 1023							
dnat	IPv4 DNAT address used for multicast destination addresses.	ipv4-address-any	Not Specified	0.0.0.0						
dstaddr <name>	Destination address objects. Destination address objects.	string	Maximum length: 79							
dstintf	Destination interface name.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default								
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (1 - 65535, default = 1).	integer	Minimum value: 0 Maximum value: 65535	65535								
id	Policy ID ((0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294	0								
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 47									
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Enable logging traffic accepted by this policy.</td></tr><tr><td>utm</td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td>disable</td><td>Disable all logging for this policy.</td></tr></table>				Option	Description	all	Enable logging traffic accepted by this policy.	utm	Log traffic that has a security profile applied to it.	disable	Disable all logging for this policy.
Option	Description											
all	Enable logging traffic accepted by this policy.											
utm	Log traffic that has a security profile applied to it.											
disable	Disable all logging for this policy.											
name	Policy name.	string	Maximum length: 35									
protocol	Integer value for the protocol type as defined by IANA (0 - 255, default = 0).	integer	Minimum value: 0 Maximum value: 255	0								
snat	Enable/disable substitution of the outgoing interface IP address for the original source IP address (called source NAT or SNAT).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source NAT.</td></tr><tr><td>disable</td><td>Disable source NAT.</td></tr></table>				Option	Description	enable	Enable source NAT.	disable	Disable source NAT.		
Option	Description											
enable	Enable source NAT.											
disable	Disable source NAT.											
snat-ip	IPv4 address to be used as the source address for NATed traffic.	ipv4-address	Not Specified	0.0.0.0								
srcaddr <name>	Source address objects. Source address objects.	string	Maximum length: 79									
srcintf	Source interface name.	string	Maximum length: 35									
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (1 - 65535, default = 1).	integer	Minimum value: 0 Maximum value: 65535	1								

Parameter	Description	Type	Size	Default						
status	Enable/disable this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.
	Option	Description								
	<i>enable</i>	Enable this policy.								
<i>disable</i>	Disable this policy.									
traffic-shaper	Traffic shaper to apply to traffic forwarded by the multicast policy.	string	Maximum length: 35							
utm-status	Enable to add an IPS security profile to the policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

config firewall multicast-policy6

Configure IPv6 multicast NAT policies.

```

config firewall multicast-policy6
  Description: Configure IPv6 multicast NAT policies.
  edit <id>
    set action [accept|deny]
    set auto-asic-offload [enable|disable]
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set dstintf {string}
    set end-port {integer}
    set ips-sensor {string}
    set logtraffic [all|utm|...]
    set name {string}
    set protocol {integer}
    set srcaddr <name1>, <name2>, ...
    set srcintf {string}
    set start-port {integer}
    set status [enable|disable]
    set utm-status [enable|disable]
    set uuid {uuid}
  next
end

```


config firewall multicast-policy6

Parameter	Description	Type	Size	Default								
action	Accept or deny traffic matching the policy.	option	-	accept								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept.</td></tr><tr><td><i>deny</i></td><td>Deny.</td></tr></table>	Option	Description	<i>accept</i>	Accept.	<i>deny</i>	Deny.					
Option	Description											
<i>accept</i>	Accept.											
<i>deny</i>	Deny.											
auto-asic-offload	Enable/disable offloading policy traffic for hardware acceleration.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable offloading policy traffic for hardware acceleration.</td></tr><tr><td><i>disable</i></td><td>Disable offloading policy traffic for hardware acceleration.</td></tr></table>	Option	Description	<i>enable</i>	Enable offloading policy traffic for hardware acceleration.	<i>disable</i>	Disable offloading policy traffic for hardware acceleration.					
Option	Description											
<i>enable</i>	Enable offloading policy traffic for hardware acceleration.											
<i>disable</i>	Disable offloading policy traffic for hardware acceleration.											
comments	Comment.	var-string	Maximum length: 1023									
dstaddr <name>	IPv6 destination address name. Address name.	string	Maximum length: 79									
dstintf	IPv6 destination interface name.	string	Maximum length: 35									
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (1 - 65535, default = 65535).	integer	Minimum value: 0 Maximum value: 65535	65535								
id	Policy ID (0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294	0								
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 47									
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Enable logging traffic accepted by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Enable logging traffic accepted by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Enable logging traffic accepted by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											

Parameter	Description	Type	Size	Default
name	Policy name.	string	Maximum length: 35	
protocol	Integer value for the protocol type as defined by IANA (0 - 255, default = 0).	integer	Minimum value: 0 Maximum value: 255	
srcaddr <name>	IPv6 source address name. Address name.	string	Maximum length: 79	
srcintf	IPv6 source interface name.	string	Maximum length: 35	
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (1 - 65535, default = 1).	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable this policy.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable this policy.	
	<i>disable</i>		Disable this policy.	
utm-status	Enable to add an IPS security profile to the policy.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config firewall network-service-dynamic

Configure Dynamic Network Services.

```
config firewall network-service-dynamic
  Description: Configure Dynamic Network Services.
  edit <name>
    set comment {var-string}
    set filter {var-string}
    set sdn {string}
  next
end
```

config firewall network-service-dynamic

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
filter	Match criteria filter.	var-string	Maximum length: 2047	
name	Dynamic Network Service name.	string	Maximum length: 63	
sdn	SDN connector name.	string	Maximum length: 35	

config firewall on-demand-sniffer

Configure on-demand packet sniffer.

```
config firewall on-demand-sniffer
  Description: Configure on-demand packet sniffer.
  edit <name>
    set advanced-filter {var-string}
    set hosts <host1>, <host2>, ...
    set interface {string}
    set max-packet-count {integer}
    set non-ip-packet [enable|disable]
    set ports <port1>, <port2>, ...
    set protocols <protocol1>, <protocol2>, ...
  next
end
```

config firewall on-demand-sniffer

Parameter	Description	Type	Size	Default
advanced-filter	Advanced freeform filter that will be used over existing filter settings if set. Can only be used by super admin.	var-string	Maximum length: 255	
hosts <host>	IPv4 or IPv6 hosts to filter in this traffic sniffer. IPv4 or IPv6 host.	string	Maximum length: 255	
interface	Interface name that on-demand packet sniffer will take place.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
max-packet-count	Maximum number of packets to capture per on-demand packet sniffer.	integer	Minimum value: 1 Maximum value: 20000 **	0						
name	On-demand packet sniffer name.	string	Maximum length: 35							
non-ip-packet	Include non-IP packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable non-IP packets to be included capture.</td></tr><tr><td>disable</td><td>Disable non-IP packets to be included in capture.</td></tr></table>				Option	Description	enable	Enable non-IP packets to be included capture.	disable	Disable non-IP packets to be included in capture.
Option	Description									
enable	Enable non-IP packets to be included capture.									
disable	Disable non-IP packets to be included in capture.									
ports <port>	Ports to filter for in this traffic sniffer. Port to filter in this traffic sniffer.	integer	Minimum value: 1 Maximum value: 65536							
protocols <protocol>	Protocols to filter in this traffic sniffer. Integer value for the protocol type as defined by IANA (0 - 255).	integer	Minimum value: 0 Maximum value: 255							

** Values may differ between models.

config firewall policy

Configure IPv4/IPv6 policies.

```
config firewall policy
  Description: Configure IPv4/IPv6 policies.
  edit <policyid>
    set action [accept|deny|...]
    set anti-replay [enable|disable]
    set app-monitor [enable|disable]
    set application-list {string}
    set auth-cert {string}
    set auth-path [enable|disable]
    set auth-redirect-addr {string}
    set auto-asic-offload [enable|disable]
    set av-profile {string}
    set block-notification [enable|disable]
    set captive-portal-exempt [enable|disable]
    set capture-packet [enable|disable]
```

```

set casb-profile {string}
set comments {var-string}
set custom-log-fields <field-id1>, <field-id2>, ...
set decrypted-traffic-mirror {string}
set delay-tcp-npu-session [enable|disable]
set diameter-filter-profile {string}
set diffserv-copy [enable|disable]
set diffserv-forward [enable|disable]
set diffserv-reverse [enable|disable]
set diffservcode-forward {user}
set diffservcode-rev {user}
set disclaimer [enable|disable]
set dlp-profile {string}
set dnsfilter-profile {string}
set dsri [enable|disable]
set dstaddr <name1>, <name2>, ...
set dstaddr-negate [enable|disable]
set dstaddr6 <name1>, <name2>, ...
set dstaddr6-negate [enable|disable]
set dstintf <name1>, <name2>, ...
set dynamic-shaping [enable|disable]
set email-collect [enable|disable]
set emailfilter-profile {string}
set fec [enable|disable]
set file-filter-profile {string}
set firewall-session-dirty [check-all|check-new]
set fixedport [enable|disable]
set fsso-agent-for-ntlm {string}
set fsso-groups <name1>, <name2>, ...
set geoip-anycast [enable|disable]
set geoip-match [physical-location|registered-location]
set groups <name1>, <name2>, ...
set http-policy-redirect [enable|disable|...]
set icap-profile {string}
set identity-based-route {string}
set inbound [enable|disable]
set inspection-mode [proxy|flow]
set internet-service [enable|disable]
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-name <name1>, <name2>, ...
set internet-service-negate [enable|disable]
set internet-service-src [enable|disable]
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-name <name1>, <name2>, ...
set internet-service-src-negate [enable|disable]
set internet-service6 [enable|disable]
set internet-service6-custom <name1>, <name2>, ...
set internet-service6-custom-group <name1>, <name2>, ...

```

```

set internet-service6-group <name1>, <name2>, ...
set internet-service6-name <name1>, <name2>, ...
set internet-service6-negate [enable|disable]
set internet-service6-src [enable|disable]
set internet-service6-src-custom <name1>, <name2>, ...
set internet-service6-src-custom-group <name1>, <name2>, ...
set internet-service6-src-group <name1>, <name2>, ...
set internet-service6-src-name <name1>, <name2>, ...
set internet-service6-src-negate [enable|disable]
set ippool [enable|disable]
set ips-sensor {string}
set ips-voip-filter {string}
set log-http-transaction [enable|disable]
set logtraffic [all|utm|...]
set logtraffic-start [enable|disable]
set match-vip [enable|disable]
set match-vip-only [enable|disable]
set name {string}
set nat [enable|disable]
set nat46 [enable|disable]
set nat64 [enable|disable]
set natinbound [enable|disable]
set natip {ipv4-classnet}
set natoutbound [enable|disable]
set network-service-dynamic <name1>, <name2>, ...
set network-service-src-dynamic <name1>, <name2>, ...
set np-acceleration [enable|disable]
set ntlm [enable|disable]
set ntlm-enabled-browsers <user-agent-string1>, <user-agent-string2>, ...
set ntlm-guest [enable|disable]
set outbound [enable|disable]
set passive-wan-health-measurement [enable|disable]
set pcp-inbound [enable|disable]
set pcp-outbound [enable|disable]
set pcp-poolname <name1>, <name2>, ...
set per-ip-shaper {string}
set permit-any-host [enable|disable]
set permit-stun-host [enable|disable]
set policy-expiry [enable|disable]
set policy-expiry-date {datetime}
set policy-expiry-date-utc {user}
set poolname <name1>, <name2>, ...
set poolname6 <name1>, <name2>, ...
set port-preserve [enable|disable]
set port-random [enable|disable]
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set radius-ip-auth-bypass [enable|disable]
set radius-mac-auth-bypass [enable|disable]
set redirect-url {var-string}
set replacemsg-override-group {string}

```

```
set reputation-direction [source|destination]
set reputation-direction6 [source|destination]
set reputation-minimum {integer}
set reputation-minimum6 {integer}
set rtp-addr <name1>, <name2>, ...
set rtp-nat [disable|enable]
set schedule {string}
set schedule-timeout [enable|disable]
set sctp-filter-profile {string}
set send-deny-packet [disable|enable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set session-ttl {user}
set sgt <id1>, <id2>, ...
set sgt-check [enable|disable]
set src-vendor-mac <id1>, <id2>, ...
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcaddr6 <name1>, <name2>, ...
set srcaddr6-negate [enable|disable]
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssh-policy-redirect [enable|disable]
set ssl-ssh-profile {string}
set status [enable|disable]
set tcp-mss-receiver {integer}
set tcp-mss-sender {integer}
set tcp-session-without-syn [all|data-only|...]
set telemetry-profile {string}
set timeout-send-rst [enable|disable]
set tos {user}
set tos-mask {user}
set tos-negate [enable|disable]
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set users <name1>, <name2>, ...
set utm-status [enable|disable]
set uuid {uuid}
set videofilter-profile {string}
set virtual-patch-profile {string}
set vlan-cos-fwd {integer}
set vlan-cos-rev {integer}
set vlan-filter {user}
set voip-profile {string}
set vpntunnel {string}
set waf-profile {string}
set wanopt [enable|disable]
set wanopt-detection [active|passive|...]
set wanopt-passive-opt [default|transparent|...]
set wanopt-peer {string}
set wanopt-profile {string}
set wccp [enable|disable]
```

```

set webcache [enable|disable]
set webcache-https [disable|enable]
set webfilter-profile {string}
set webproxy-forward-server {string}
set webproxy-profile {string}
set ztna-device-ownership [enable|disable]
set ztna-ems-tag <name1>, <name2>, ...
set ztna-ems-tag-negate [enable|disable]
set ztna-ems-tag-secondary <name1>, <name2>, ...
set ztna-geo-tag <name1>, <name2>, ...
set ztna-policy-redirect [enable|disable]
set ztna-status [enable|disable]
set ztna-tags-match-logic [or|and]
next
end

```

config firewall policy

Parameter	Description	Type	Size	Default								
action	Policy action (accept/deny/ipsec).	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Allows session that match the firewall policy.</td></tr><tr><td><i>deny</i></td><td>Blocks sessions that match the firewall policy.</td></tr><tr><td><i>ipsec</i></td><td>Firewall policy becomes a policy-based IPsec VPN policy.</td></tr></table>	Option	Description	<i>accept</i>	Allows session that match the firewall policy.	<i>deny</i>	Blocks sessions that match the firewall policy.	<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.			
Option	Description											
<i>accept</i>	Allows session that match the firewall policy.											
<i>deny</i>	Blocks sessions that match the firewall policy.											
<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.											
anti-replay	Enable/disable anti-replay check.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anti-replay check.</td></tr><tr><td><i>disable</i></td><td>Disable anti-replay check.</td></tr></table>	Option	Description	<i>enable</i>	Enable anti-replay check.	<i>disable</i>	Disable anti-replay check.					
Option	Description											
<i>enable</i>	Enable anti-replay check.											
<i>disable</i>	Disable anti-replay check.											
app-monitor	Enable/disable application TCP metrics in session logs.When enabled, auto-asic-offload is disabled.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TCP metrics in session logs.</td></tr><tr><td><i>disable</i></td><td>Disable TCP metrics in session logs.</td></tr></table>	Option	Description	<i>enable</i>	Enable TCP metrics in session logs.	<i>disable</i>	Disable TCP metrics in session logs.					
Option	Description											
<i>enable</i>	Enable TCP metrics in session logs.											
<i>disable</i>	Disable TCP metrics in session logs.											
application-list	Name of an existing Application list.	string	Maximum length: 47									
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default
auth-path	Enable/disable authentication-based routing.	option	-	disable
	Option Description			
	<i>enable</i>	Enable authentication-based routing.		
	<i>disable</i>	Disable authentication-based routing.		
auth-redirect-addr	HTTP-to-HTTPS redirect address for firewall authentication.	string	Maximum length: 63	
auto-asic-offload	Enable/disable policy traffic ASIC offloading.	option	-	enable
	Option Description			
	<i>enable</i>	Enable auto ASIC offloading.		
	<i>disable</i>	Disable ASIC offloading.		
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 47	
block-notification	Enable/disable block notification.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
captive-portal-exempt	Enable to exempt some users from the captive portal.	option	-	disable
	Option Description			
	<i>enable</i>	Enable exemption of captive portal.		
	<i>disable</i>	Disable exemption of captive portal.		
capture-packet *	Enable/disable capture packets.	option	-	disable
	Option Description			
	<i>enable</i>	Enable capture packets.		
	<i>disable</i>	Disable capture packets.		
casb-profile	Name of an existing CASB profile.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 1023							
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35							
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
delay-tcp-npu-session	Enable TCP NPU session delay to guarantee packet order of 3-way handshake.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.</td></tr><tr><td><i>disable</i></td><td>Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.</td></tr></table>				Option	Description	<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.	<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.
Option	Description									
<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.									
<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.									
diameter-filter-profile	Name of an existing Diameter filter profile.	string	Maximum length: 47							
diffserv-copy	Enable to copy packet's DiffServ values from session's original direction to its reply direction.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DSCP copy.</td></tr><tr><td><i>disable</i></td><td>Disable DSCP copy.</td></tr></table>				Option	Description	<i>enable</i>	Enable DSCP copy.	<i>disable</i>	Disable DSCP copy.
Option	Description									
<i>enable</i>	Enable DSCP copy.									
<i>disable</i>	Disable DSCP copy.									
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting forward (original) traffic Diffserv.</td></tr><tr><td><i>disable</i></td><td>Disable setting forward (original) traffic Diffserv.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting forward (original) traffic Diffserv.	<i>disable</i>	Disable setting forward (original) traffic Diffserv.
Option	Description									
<i>enable</i>	Enable setting forward (original) traffic Diffserv.									
<i>disable</i>	Disable setting forward (original) traffic Diffserv.									
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.		
	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.		
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified	
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified	
disclaimer	Enable/disable user authentication disclaimer.	option	-	disable
	Option Description			
	<i>enable</i>	Enable user authentication disclaimer.		
	<i>disable</i>	Disable user authentication disclaimer.		
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 47	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 47	
dsri	Enable DSRI to ignore HTTP server responses.	option	-	disable
	Option Description			
	<i>enable</i>	Enable DSRI.		
	<i>disable</i>	Disable DSRI.		
dstaddr <name>	Destination IPv4 address and address group names. Address name.	string	Maximum length: 79	
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable
	Option Description			
	<i>enable</i>	Enable destination address negate.		
	<i>disable</i>	Disable destination address negate.		
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
dstaddr6-negate	When enabled dstaddr6 specifies what the destination address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPv6 destination address negate.</td></tr><tr><td>disable</td><td>Disable IPv6 destination address negate.</td></tr></table>	Option	Description	enable	Enable IPv6 destination address negate.	disable	Disable IPv6 destination address negate.			
Option	Description									
enable	Enable IPv6 destination address negate.									
disable	Disable IPv6 destination address negate.									
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79							
dynamic-shaping	Enable/disable dynamic RADIUS defined traffic shaping.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dynamic RADIUS defined traffic shaping.</td></tr><tr><td>disable</td><td>Disable dynamic RADIUS defined traffic shaping.</td></tr></table>	Option	Description	enable	Enable dynamic RADIUS defined traffic shaping.	disable	Disable dynamic RADIUS defined traffic shaping.			
Option	Description									
enable	Enable dynamic RADIUS defined traffic shaping.									
disable	Disable dynamic RADIUS defined traffic shaping.									
email-collect	Enable/disable email collection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable email collection.</td></tr><tr><td>disable</td><td>Disable email collection.</td></tr></table>	Option	Description	enable	Enable email collection.	disable	Disable email collection.			
Option	Description									
enable	Enable email collection.									
disable	Disable email collection.									
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 47							
fec	Enable/disable Forward Error Correction on traffic matching this policy on a FEC device.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Forward Error Correction.</td></tr><tr><td>disable</td><td>Disable Forward Error Correction.</td></tr></table>	Option	Description	enable	Enable Forward Error Correction.	disable	Disable Forward Error Correction.			
Option	Description									
enable	Enable Forward Error Correction.									
disable	Disable Forward Error Correction.									
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 47							
firewall-session-dirty	How to handle sessions if the configuration of this firewall policy changes.	option	-	check-all						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>check-all</i>	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.		
	<i>check-new</i>	Continue to allow sessions already accepted by this policy.		
fixedport	Enable to prevent source NAT from changing a session's source port.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35	
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511	
geoip-anycast	Enable/disable recognition of anycast IP addresses using the geography IP database.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable recognition of anycast IP addresses using the geography IP database.		
	<i>disable</i>	Disable recognition of anycast IP addresses using the geography IP database.		
geoip-match	Match geography address based either on its physical location or registered location.	option	-	physical-location
	Option	Description		
	<i>physical-location</i>	Match geography address to its physical location using the geography IP database.		
	<i>registered-location</i>	Match geography address to its registered location using the geography IP database.		
groups <name>	Names of user groups that can authenticate with this policy. Group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default								
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP(S) policy redirect.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP(S) policy redirect.</td></tr><tr><td><i>legacy</i></td><td>Enable HTTP(S) policy redirect (for preserving old behavior, not recommended for new setups).</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP(S) policy redirect.	<i>disable</i>	Disable HTTP(S) policy redirect.	<i>legacy</i>	Enable HTTP(S) policy redirect (for preserving old behavior, not recommended for new setups).			
Option	Description											
<i>enable</i>	Enable HTTP(S) policy redirect.											
<i>disable</i>	Disable HTTP(S) policy redirect.											
<i>legacy</i>	Enable HTTP(S) policy redirect (for preserving old behavior, not recommended for new setups).											
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 47									
identity-based-route	Name of identity-based routing rule.	string	Maximum length: 35									
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-	flow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>proxy</i></td><td>Proxy based inspection.</td></tr><tr><td><i>flow</i></td><td>Flow based inspection.</td></tr></table>	Option	Description	<i>proxy</i>	Proxy based inspection.	<i>flow</i>	Flow based inspection.					
Option	Description											
<i>proxy</i>	Proxy based inspection.											
<i>flow</i>	Flow based inspection.											
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.					
Option	Description											
<i>enable</i>	Enable use of Internet Services in policy.											
<i>disable</i>	Disable use of Internet Services in policy.											
internet-service-custom<name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default						
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79							
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service match.</td></tr></table>				Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.
Option	Description									
<i>enable</i>	Enable negated Internet Service match.									
<i>disable</i>	Disable negated Internet Service match.									
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services source in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services source in policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of Internet Services source in policy.	<i>disable</i>	Disable use of Internet Services source in policy.
Option	Description									
<i>enable</i>	Enable use of Internet Services source in policy.									
<i>disable</i>	Disable use of Internet Services source in policy.									
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated Internet Service source match.</td></tr><tr><td>disable</td><td>Disable negated Internet Service source match.</td></tr></table>	Option	Description	enable	Enable negated Internet Service source match.	disable	Disable negated Internet Service source match.			
Option	Description									
enable	Enable negated Internet Service source match.									
disable	Disable negated Internet Service source match.									
internet-service6	Enable/disable use of IPv6 Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of IPv6 Internet Services in policy.</td></tr><tr><td>disable</td><td>Disable use of IPv6 Internet Services in policy.</td></tr></table>	Option	Description	enable	Enable use of IPv6 Internet Services in policy.	disable	Disable use of IPv6 Internet Services in policy.			
Option	Description									
enable	Enable use of IPv6 Internet Services in policy.									
disable	Disable use of IPv6 Internet Services in policy.									
internet-service6-custom <name>	Custom IPv6 Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service6-custom-group <name>	Custom Internet Service6 group name. Custom Internet Service6 group name.	string	Maximum length: 79							
internet-service6-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service6-name <name>	IPv6 Internet Service name. IPv6 Internet Service name.	string	Maximum length: 79							
internet-service6-negate	When enabled internet-service6 specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated IPv6 Internet Service match.</td></tr><tr><td>disable</td><td>Disable negated IPv6 Internet Service match.</td></tr></table>	Option	Description	enable	Enable negated IPv6 Internet Service match.	disable	Disable negated IPv6 Internet Service match.			
Option	Description									
enable	Enable negated IPv6 Internet Service match.									
disable	Disable negated IPv6 Internet Service match.									
internet-service6-src	Enable/disable use of IPv6 Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable use of IPv6 Internet Services source in policy.		
	<i>disable</i>	Disable use of IPv6 Internet Services source in policy.		
internet-service6-src-custom <name>	Custom IPv6 Internet Service source name. Custom Internet Service name.	string	Maximum length: 79	
internet-service6-src-custom-group <name>	Custom Internet Service6 source group name. Custom Internet Service6 group name.	string	Maximum length: 79	
internet-service6-src-group <name>	Internet Service6 source group name. Internet Service group name.	string	Maximum length: 79	
internet-service6-src-name <name>	IPv6 Internet Service source name. Internet Service name.	string	Maximum length: 79	
internet-service6-src-negate	When enabled internet-service6-src specifies what the service must NOT be.	option	-	disable
	Option Description			
	<i>enable</i>	Enable negated IPv6 Internet Service source match.		
	<i>disable</i>	Disable negated IPv6 Internet Service source match.		
ippool	Enable to use IP Pools for source NAT.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 47	
ips-voip-filter	Name of an existing VoIP (ips) profile.	string	Maximum length: 47	
log-http-transaction	Enable/disable HTTP transaction log.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP transaction log.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP transaction log.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP transaction log.	<i>disable</i>	Disable HTTP transaction log.					
	Option	Description										
	<i>enable</i>	Enable HTTP transaction log.										
<i>disable</i>	Disable HTTP transaction log.											
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
	Option	Description										
	<i>all</i>	Log all sessions accepted or denied by this policy.										
	<i>utm</i>	Log traffic that has a security profile applied to it.										
<i>disable</i>	Disable all logging for this policy.											
logtraffic-start	Record logs when a session starts.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
match-vip	Enable to match packets that have had their destination addresses changed by a VIP.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Match DNATed packet.</td></tr><tr><td><i>disable</i></td><td>Do not match DNATed packet.</td></tr></table>	Option	Description	<i>enable</i>	Match DNATed packet.	<i>disable</i>	Do not match DNATed packet.					
	Option	Description										
	<i>enable</i>	Match DNATed packet.										
<i>disable</i>	Do not match DNATed packet.											
match-vip-only	Enable/disable matching of only those packets that have had their destination addresses changed by a VIP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable matching of only those packets that have had their destination addresses changed by a VIP.</td></tr><tr><td><i>disable</i></td><td>Disable matching of only those packets that have had their destination addresses changed by a VIP.</td></tr></table>	Option	Description	<i>enable</i>	Enable matching of only those packets that have had their destination addresses changed by a VIP.	<i>disable</i>	Disable matching of only those packets that have had their destination addresses changed by a VIP.					
	Option	Description										
	<i>enable</i>	Enable matching of only those packets that have had their destination addresses changed by a VIP.										
<i>disable</i>	Disable matching of only those packets that have had their destination addresses changed by a VIP.											
name	Policy name.	string	Maximum length: 35									
nat	Enable/disable source NAT.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
nat46	Enable/disable NAT46.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable NAT46.		
	<i>disable</i>	Disable NAT46.		
nat64	Enable/disable NAT64.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable NAT64.		
	<i>disable</i>	Disable NAT64.		
natinbound	Policy-based IPsec VPN: apply destination NAT to inbound traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
natip	Policy-based IPsec VPN: source NAT IP address for outgoing traffic.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
natoutbound	Policy-based IPsec VPN: apply source NAT to outbound traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
network-service-dynamic <name>	Dynamic Network Service name. Dynamic Network Service name.	string	Maximum length: 79	
network-service-src-dynamic <name>	Dynamic Network Service source name. Dynamic Network Service name.	string	Maximum length: 79	
np-acceleration *	Enable/disable UTM Network Processor acceleration.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable UTM Network Processor acceleration.		
	<i>disable</i>	Disable UTM Network Processor acceleration.		
ntlm	Enable/disable NTLM authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ntlm-enabled-browsers <user-agent-string>	HTTP-User-Agent value of supported browsers. User agent string.	string	Maximum length: 79	
ntlm-guest	Enable/disable NTLM guest user access.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
passive-wan-health-measurement	Enable/disable passive WAN health measurement. When enabled, auto-asic-offload is disabled.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Passive WAN health measurement.		
	<i>disable</i>	Disable Passive WAN health measurement.		
pcp-inbound	Enable/disable PCP inbound DNAT.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable PCP inbound DNAT.		
	<i>disable</i>	Disable PCP inbound DNAT.		
pcp-outbound	Enable/disable PCP outbound SNAT.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PCP outbound SNAT.		
	<i>disable</i>	Disable PCP outbound SNAT.		
pcp-poolname <name>	PCP pool names. PCP pool name.	string	Maximum length: 79	
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35	
permit-any-host	Accept UDP packets from any host.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-stun-host	Accept UDP packets from any Session Traversal Utilities for NAT (STUN) host.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
policy-expiry	Enable/disable policy expiry.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable policy expiry.		
	<i>disable</i>	Disable policy expiry.		
policy-expiry-date	Policy expiry date (YYYY-MM-DD HH:MM:SS).	datetime	Not Specified	0000-00-00 00:00:00
policy-expiry-date-utc	Policy expiry date and time, in epoch format.	user	Not Specified	

Parameter	Description	Type	Size	Default						
policyid	Policy ID (0 - 4294967294).	integer	Minimum value: 0 0 Maximum value: 4294967294							
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79							
poolname6 <name>	IPv6 pool names. IPv6 pool name.	string	Maximum length: 79							
port-preserve	Enable/disable preservation of the original source port from source NAT if it has not been used.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Use the original source port if it has not been used.</td></tr><tr><td>disable</td><td>Source NAT always changes the source port.</td></tr></table>				Option	Description	enable	Use the original source port if it has not been used.	disable	Source NAT always changes the source port.
Option	Description									
enable	Use the original source port if it has not been used.									
disable	Source NAT always changes the source port.									
port-random	Enable/disable random source port selection for source NAT.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable random source port selection for source NAT.</td></tr><tr><td>disable</td><td>Disable random source port selection for source NAT.</td></tr></table>				Option	Description	enable	Enable random source port selection for source NAT.	disable	Disable random source port selection for source NAT.
Option	Description									
enable	Enable random source port selection for source NAT.									
disable	Disable random source port selection for source NAT.									
profile-group	Name of profile group.	string	Maximum length: 47							
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 47	default						
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>single</td><td>Do not allow security profile groups.</td></tr><tr><td>group</td><td>Allow security profile groups.</td></tr></table>				Option	Description	single	Do not allow security profile groups.	group	Allow security profile groups.
Option	Description									
single	Do not allow security profile groups.									
group	Allow security profile groups.									
radius-ip-auth-bypass	Enable IP authentication bypass. The bypassed IP address must be received from RADIUS server.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP authentication bypass.</td></tr><tr><td><i>disable</i></td><td>Disable IP authentication bypass.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP authentication bypass.	<i>disable</i>	Disable IP authentication bypass.			
	Option	Description								
	<i>enable</i>	Enable IP authentication bypass.								
<i>disable</i>	Disable IP authentication bypass.									
radius-mac-auth-bypass	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MAC authentication bypass.</td></tr><tr><td><i>disable</i></td><td>Disable MAC authentication bypass.</td></tr></table>	Option	Description	<i>enable</i>	Enable MAC authentication bypass.	<i>disable</i>	Disable MAC authentication bypass.			
	Option	Description								
	<i>enable</i>	Enable MAC authentication bypass.								
<i>disable</i>	Disable MAC authentication bypass.									
redirect-url	URL users are directed to after seeing and accepting the disclaimer or authenticating.	var-string	Maximum length: 1023							
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35							
reputation-direction	Direction of the initial traffic for reputation to take effect.	option	-	destination						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>source</i></td><td>Check reputation for source address.</td></tr><tr><td><i>destination</i></td><td>Check reputation for destination address.</td></tr></table>	Option	Description	<i>source</i>	Check reputation for source address.	<i>destination</i>	Check reputation for destination address.			
	Option	Description								
	<i>source</i>	Check reputation for source address.								
<i>destination</i>	Check reputation for destination address.									
reputation-direction6	Direction of the initial traffic for IPv6 reputation to take effect.	option	-	destination						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>source</i></td><td>Check reputation for IPv6 source address.</td></tr><tr><td><i>destination</i></td><td>Check reputation for IPv6 destination address.</td></tr></table>	Option	Description	<i>source</i>	Check reputation for IPv6 source address.	<i>destination</i>	Check reputation for IPv6 destination address.			
	Option	Description								
	<i>source</i>	Check reputation for IPv6 source address.								
<i>destination</i>	Check reputation for IPv6 destination address.									
reputation-minimum	Minimum Reputation to take action.	integer	Minimum value: 0 0 Maximum value: 4294967295							
reputation-minimum6	IPv6 Minimum Reputation to take action.	integer	Minimum value: 0 0 Maximum value: 4294967295							
rtp-addr <name>	Address names if this is an RTP NAT policy.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
	Address name.									
rtp-nat	Enable Real Time Protocol (RTP) NAT.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable setting.</td></tr><tr><td>enable</td><td>Enable setting.</td></tr></table>	Option	Description	disable	Disable setting.	enable	Enable setting.			
Option	Description									
disable	Disable setting.									
enable	Enable setting.									
schedule	Schedule name.	string	Maximum length: 35							
schedule-timeout	Enable to force current sessions to end when the schedule object times out. Disable allows them to end from inactivity.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable schedule timeout.</td></tr><tr><td>disable</td><td>Disable schedule timeout.</td></tr></table>	Option	Description	enable	Enable schedule timeout.	disable	Disable schedule timeout.			
Option	Description									
enable	Enable schedule timeout.									
disable	Disable schedule timeout.									
sctp-filter-profile	Name of an existing SCTP filter profile.	string	Maximum length: 47							
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable deny-packet sending.</td></tr><tr><td>enable</td><td>Enable deny-packet sending.</td></tr></table>	Option	Description	disable	Disable deny-packet sending.	enable	Enable deny-packet sending.			
Option	Description									
disable	Disable deny-packet sending.									
enable	Enable deny-packet sending.									
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79							
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated service match.</td></tr><tr><td>disable</td><td>Disable negated service match.</td></tr></table>	Option	Description	enable	Enable negated service match.	disable	Disable negated service match.			
Option	Description									
enable	Enable negated service match.									
disable	Disable negated service match.									
session-ttl	TTL in seconds for sessions accepted by this policy (0 means use the system default session TTL).	user	Not Specified							

Parameter	Description	Type	Size	Default
sgt <id>	Security group tags. Security group tag (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	
sgt-check	Enable/disable security group tags (SGT) check.	option	-	disable
	Option	Description		
	enable	Enable SGT check.		
	disable	Disable SGT check.		
src-vendor-mac <id>	Vendor MAC source ID. Vendor MAC ID.	integer	Minimum value: 0 Maximum value: 4294967295	
srcaddr <name>	Source IPv4 address and address group names. Address name.	string	Maximum length: 79	
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable
	Option	Description		
	enable	Enable source address negate.		
	disable	Disable source address negate.		
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79	
srcaddr6-negate	When enabled srcaddr6 specifies what the source address must NOT be.	option	-	disable
	Option	Description		
	enable	Enable IPv6 source address negate.		
	disable	Disable IPv6 source address negate.		
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default								
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH policy redirect.</td></tr><tr><td><i>disable</i></td><td>Disable SSH policy redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSH policy redirect.	<i>disable</i>	Disable SSH policy redirect.					
Option	Description											
<i>enable</i>	Enable SSH policy redirect.											
<i>disable</i>	Disable SSH policy redirect.											
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 47	no-inspection								
status	Enable or disable this policy.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 0 Maximum value: 65535									
tcp-mss-sender	Sender TCP maximum segment size (MSS).	integer	Minimum value: 0 0 Maximum value: 65535									
tcp-session-without-syn	Enable/disable creation of TCP session without SYN flag.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Enable TCP session without SYN.</td></tr><tr><td><i>data-only</i></td><td>Enable TCP session data only.</td></tr><tr><td><i>disable</i></td><td>Disable TCP session without SYN.</td></tr></table>	Option	Description	<i>all</i>	Enable TCP session without SYN.	<i>data-only</i>	Enable TCP session data only.	<i>disable</i>	Disable TCP session without SYN.			
Option	Description											
<i>all</i>	Enable TCP session without SYN.											
<i>data-only</i>	Enable TCP session data only.											
<i>disable</i>	Disable TCP session without SYN.											
telemetry-profile *	Name of an existing telemetry profile.	string	Maximum length: 47									
timeout-send-rst	Enable/disable sending RST packets when TCP sessions expire.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of RST packet upon TCP session expiration.</td></tr><tr><td><i>disable</i></td><td>Disable sending of RST packet upon TCP session expiration.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of RST packet upon TCP session expiration.	<i>disable</i>	Disable sending of RST packet upon TCP session expiration.					
Option	Description											
<i>enable</i>	Enable sending of RST packet upon TCP session expiration.											
<i>disable</i>	Disable sending of RST packet upon TCP session expiration.											
tos	ToS (Type of Service) value used for comparison.	user	Not Specified									

Parameter	Description	Type	Size	Default
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified	
tos-negate	Enable negated TOS match.	option	-	disable
	Option Description			
	enable Enable TOS match negate.			
	disable Disable TOS match negate.			
traffic-shaper	Traffic shaper.	string	Maximum length: 35	
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35	
users <name>	Names of individual users that can authenticate with this policy. Names of individual users that can authenticate with this policy.	string	Maximum length: 79	
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-	disable
	Option Description			
	enable Enable setting.			
	disable Disable setting.			
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 47	
virtual-patch-profile	Name of an existing virtual-patch profile.	string	Maximum length: 47	
vlan-cos-fwd	VLAN forward direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7	255
vlan-cos-rev	VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7	255
vlan-filter	VLAN ranges to allow	user	Not Specified	

Parameter	Description	Type	Size	Default								
voip-profile	Name of an existing VoIP (voipd) profile.	string	Maximum length: 47									
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35									
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 47									
wanopt *	Enable/disable WAN optimization.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
wanopt-detection *	WAN optimization auto-detection mode.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Active WAN optimization peer auto-detection.</td></tr><tr><td><i>passive</i></td><td>Passive WAN optimization peer auto-detection.</td></tr><tr><td><i>off</i></td><td>Turn off WAN optimization peer auto-detection.</td></tr></table>	Option	Description	<i>active</i>	Active WAN optimization peer auto-detection.	<i>passive</i>	Passive WAN optimization peer auto-detection.	<i>off</i>	Turn off WAN optimization peer auto-detection.			
Option	Description											
<i>active</i>	Active WAN optimization peer auto-detection.											
<i>passive</i>	Passive WAN optimization peer auto-detection.											
<i>off</i>	Turn off WAN optimization peer auto-detection.											
wanopt-passive-opt *	WAN optimization passive mode options. This option decides what IP address will be used to connect server.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Allow client side WAN opt peer to decide.</td></tr><tr><td><i>transparent</i></td><td>Use address of client to connect to server.</td></tr><tr><td><i>non-transparent</i></td><td>Use local FortiGate address to connect to server.</td></tr></table>	Option	Description	<i>default</i>	Allow client side WAN opt peer to decide.	<i>transparent</i>	Use address of client to connect to server.	<i>non-transparent</i>	Use local FortiGate address to connect to server.			
Option	Description											
<i>default</i>	Allow client side WAN opt peer to decide.											
<i>transparent</i>	Use address of client to connect to server.											
<i>non-transparent</i>	Use local FortiGate address to connect to server.											
wanopt-peer *	WAN optimization peer.	string	Maximum length: 35									
wanopt-profile *	WAN optimization profile.	string	Maximum length: 35									
wccp	Enable/disable forwarding traffic matching this policy to a configured WCCP server.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable WCCP setting.		
	<i>disable</i>	Disable WCCP setting.		
webcache *	Enable/disable web cache.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
webcache-https *	Enable/disable web cache for HTTPS.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable web cache for HTTPS.		
	<i>enable</i>	Enable web cache for HTTPS.		
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 47	
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63	
webproxy-profile	Webproxy profile name.	string	Maximum length: 63	
ztna-device-ownership	Enable/disable zero trust device ownership.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ZTNA device ownership check.		
	<i>disable</i>	Disable ZTNA device ownership check.		
ztna-ems-tag <name>	Source ztna-ems-tag names. Address name.	string	Maximum length: 79	
ztna-ems-tag-negate	When enabled ztna-ems-tag specifies what the tags must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ZTNA EMS tags negate.		
	<i>disable</i>	Disable ZTNA EMS tags negate.		

Parameter	Description	Type	Size	Default						
ztna-ems-tag-secondary <name>	Source ztna-ems-tag-secondary names. Address name.	string	Maximum length: 79							
ztna-geo-tag <name>	Source ztna-geo-tag names. Address name.	string	Maximum length: 79							
ztna-policy-redirect	Redirect ZTNA traffic to matching Access-Proxy proxy-policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ZTNA proxy-policy redirect.</td></tr><tr><td><i>disable</i></td><td>Disable ZTNA proxy-policy redirect.</td></tr></table>				Option	Description	<i>enable</i>	Enable ZTNA proxy-policy redirect.	<i>disable</i>	Disable ZTNA proxy-policy redirect.
Option	Description									
<i>enable</i>	Enable ZTNA proxy-policy redirect.									
<i>disable</i>	Disable ZTNA proxy-policy redirect.									
ztna-status	Enable/disable zero trust access.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero trust network access.</td></tr><tr><td><i>disable</i></td><td>Disable zero trust network access.</td></tr></table>				Option	Description	<i>enable</i>	Enable zero trust network access.	<i>disable</i>	Disable zero trust network access.
Option	Description									
<i>enable</i>	Enable zero trust network access.									
<i>disable</i>	Disable zero trust network access.									
ztna-tags-match-logic	ZTNA tag matching logic.	option	-	or						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>or</i></td><td>Match ZTNA tags using a logical OR operator.</td></tr><tr><td><i>and</i></td><td>Match ZTNA tags using a logical AND operator.</td></tr></table>				Option	Description	<i>or</i>	Match ZTNA tags using a logical OR operator.	<i>and</i>	Match ZTNA tags using a logical AND operator.
Option	Description									
<i>or</i>	Match ZTNA tags using a logical OR operator.									
<i>and</i>	Match ZTNA tags using a logical AND operator.									

* This parameter may not exist in some models.

config firewall profile-group

Configure profile groups.

```
config firewall profile-group
  Description: Configure profile groups.
  edit <name>
    set application-list {string}
    set av-profile {string}
    set casb-profile {string}
    set diameter-filter-profile {string}
    set dlp-profile {string}
    set dnsfilter-profile {string}
    set emailfilter-profile {string}
    set file-filter-profile {string}
```

```

    set icap-profile {string}
    set ips-sensor {string}
    set ips-voip-filter {string}
    set profile-protocol-options {string}
    set sctp-filter-profile {string}
    set ssh-filter-profile {string}
    set ssl-ssh-profile {string}
    set telemetry-profile {string}
    set videofilter-profile {string}
    set virtual-patch-profile {string}
    set voip-profile {string}
    set waf-profile {string}
    set webfilter-profile {string}
  next
end

```

config firewall profile-group

Parameter	Description	Type	Size	Default
application-list	Name of an existing Application list.	string	Maximum length: 47	
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 47	
casb-profile	Name of an existing CASB profile.	string	Maximum length: 47	
diameter-filter-profile	Name of an existing Diameter filter profile.	string	Maximum length: 47	
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 47	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 47	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 47	
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 47	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 47	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 47	
ips-voip-filter	Name of an existing VoIP (ips) profile.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
name	Profile group name.	string	Maximum length: 47	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 47	default
sctp-filter-profile	Name of an existing SCTP filter profile.	string	Maximum length: 47	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 47	
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 47	certificate-inspection
telemetry-profile *	Name of an existing telemetry profile.	string	Maximum length: 47	
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 47	
virtual-patch-profile	Name of an existing virtual-patch profile.	string	Maximum length: 47	
voip-profile	Name of an existing VoIP (voipd) profile.	string	Maximum length: 47	
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 47	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 47	

* This parameter may not exist in some models.

config firewall profile-protocol-options

Configure protocol options.

```

config firewall profile-protocol-options
  Description: Configure protocol options.
  edit <name>
    config cifs
      Description: Configure CIFS protocol options.
      set domain-controller {string}
      set options {option1}, {option2}, ...
      set oversize-limit {integer}
      set ports {integer}
      set scan-bzip2 [enable|disable]
      set server-credential-type [none|credential-replication|...]

```



```

config server-keytab
    Description: Server keytab.
    edit <principal>
        set keytab {string}
    next
end
set status [enable|disable]
set tcp-window-maximum {integer}
set tcp-window-minimum {integer}
set tcp-window-size {integer}
set tcp-window-type [auto-tuning|system|...]
set uncompressed-nest-limit {integer}
set uncompressed-oversize-limit {integer}
end
set comment {var-string}
config dns
    Description: Configure DNS protocol options.
    set ports {integer}
    set status [enable|disable]
end
config ftp
    Description: Configure FTP protocol options.
    set comfort-amount {integer}
    set comfort-interval {integer}
    set explicit-ftp-tls [enable|disable]
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set stream-based-uncompressed-limit {integer}
    set tcp-window-maximum {integer}
    set tcp-window-minimum {integer}
    set tcp-window-size {integer}
    set tcp-window-type [auto-tuning|system|...]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config http
    Description: Configure HTTP protocol options.
    set address-ip-rating [enable|disable]
    set block-page-status-code {integer}
    set comfort-amount {integer}
    set comfort-interval {integer}
    set domain-fronting [allow|block|...]
    set h2c [enable|disable]
    set http-0 9 [allow|block]
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}

```

```

    set ports {integer}
    set post-lang {option1}, {option2}, ...
    set proxy-after-tcp-handshake [enable|disable]
    set range-block [disable|enable]
    set retry-count {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set stream-based-uncompressed-limit {integer}
    set streaming-content-bypass [enable|disable]
    set strip-x-forwarded-for [disable|enable]
    set switching-protocols [bypass|block]
    set tcp-window-maximum {integer}
    set tcp-window-minimum {integer}
    set tcp-window-size {integer}
    set tcp-window-type [auto-tuning|system|...]
    set tunnel-non-http [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
    set unknown-content-encoding [block|inspect|...]
    set unknown-http-version [reject|tunnel|...]
    set verify-dns-for-policy-matching [enable|disable]
end
config imap
    Description: Configure IMAP protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config mail-signature
    Description: Configure Mail signature.
    set signature {string}
    set status [disable|enable]
end
config mapi
    Description: Configure MAPI protocol options.
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set scan-bzip2 [enable|disable]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config nntp

```

```

    Description: Configure NNTP protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set scan-bzip2 [enable|disable]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
set oversize-log [disable|enable]
config pop3
    Description: Configure POP3 protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
set replacemsg-group {string}
set rpc-over-http [enable|disable]
config smtp
    Description: Configure SMTP protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set scan-bzip2 [enable|disable]
    set server-busy [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config ssh
    Description: Configure SFTP and SCP protocol options.
    set comfort-amount {integer}
    set comfort-interval {integer}
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set stream-based-uncompressed-limit {integer}
    set tcp-window-maximum {integer}
    set tcp-window-minimum {integer}

```

```

        set tcp-window-size {integer}
        set tcp-window-type [auto-tuning|system|...]
        set uncompressed-nest-limit {integer}
        set uncompressed-oversize-limit {integer}
    end
    set switching-protocols-log [disable|enable]
next
end

```

config firewall profile-protocol-options

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
name	Name.	string	Maximum length: 47							
oversize-log	Enable/disable logging for antivirus oversize file blocking.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging for antivirus oversize file blocking.</td></tr><tr><td>enable</td><td>Enable logging for antivirus oversize file blocking.</td></tr></table>	Option	Description	disable	Disable logging for antivirus oversize file blocking.	enable	Enable logging for antivirus oversize file blocking.			
Option	Description									
disable	Disable logging for antivirus oversize file blocking.									
enable	Enable logging for antivirus oversize file blocking.									
replacemsg-group	Name of the replacement message group to be used.	string	Maximum length: 35							
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable inspection of RPC over HTTP.</td></tr><tr><td>disable</td><td>Disable inspection of RPC over HTTP.</td></tr></table>	Option	Description	enable	Enable inspection of RPC over HTTP.	disable	Disable inspection of RPC over HTTP.			
Option	Description									
enable	Enable inspection of RPC over HTTP.									
disable	Disable inspection of RPC over HTTP.									
switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging for HTTP/HTTPS switching protocols.</td></tr><tr><td>enable</td><td>Enable logging for HTTP/HTTPS switching protocols.</td></tr></table>	Option	Description	disable	Disable logging for HTTP/HTTPS switching protocols.	enable	Enable logging for HTTP/HTTPS switching protocols.			
Option	Description									
disable	Disable logging for HTTP/HTTPS switching protocols.									
enable	Enable logging for HTTP/HTTPS switching protocols.									

config cifs

Parameter	Description	Type	Size	Default								
domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 63									
options	One or more options that can be applied to the session.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>oversize</td><td>Block oversized file.</td></tr></table>	Option	Description	oversize	Block oversized file.							
Option	Description											
oversize	Block oversized file.											
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10								
ports	Ports to scan for content (1 - 65535, default = 445).	integer	Minimum value: 1 Maximum value: 65535									
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
Option	Description											
enable	Enable setting.											
disable	Disable setting.											
server-credential-type	CIFS server credential type.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Credential derivation not set.</td></tr><tr><td>credential-replication</td><td>Credential derived using Replication account on Domain Controller.</td></tr><tr><td>credential-keytab</td><td>Credential derived using server keytab.</td></tr></table>	Option	Description	none	Credential derivation not set.	credential-replication	Credential derived using Replication account on Domain Controller.	credential-keytab	Credential derived using server keytab.			
Option	Description											
none	Credential derivation not set.											
credential-replication	Credential derived using Replication account on Domain Controller.											
credential-keytab	Credential derived using server keytab.											
status	Enable/disable the active status of scanning for this protocol.	option	-	enable								

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 16777216	8388608										
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 16777216	262144										
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-tuning</i></td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td><i>system</i></td><td>Use system default TCP window size for this protocol.</td></tr><tr><td><i>static</i></td><td>Manually specify TCP window size.</td></tr><tr><td><i>dynamic</i></td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>	Option	Description	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).	<i>system</i>	Use system default TCP window size for this protocol.	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
	Option	Description												
	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).												
	<i>system</i>	Use system default TCP window size for this protocol.												
<i>static</i>	Manually specify TCP window size.													
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100	12										
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10										

** Values may differ between models.

config server-keytab

Parameter	Description	Type	Size	Default
keytab	Base64 encoded keytab file containing credential of the server.	string	Maximum length: 8191	
principal	Service principal. For example, host/cifsserver.example.com@example.com.	string	Maximum length: 511	

config dns

Parameter	Description	Type	Size	Default
ports	Ports to scan for content (1 - 65535, default = 53).	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

config ftp

Parameter	Description	Type	Size	Default						
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1						
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 1 Maximum value: 900	10						
explicit-ftp-tls	Enable/disable FTP redirection for explicit FTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
options	One or more options that can be applied to the session.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>clientcomfort</i></td><td>Prevent client timeout.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file.</td></tr><tr><td><i>splice</i></td><td>Enable splice mode.</td></tr><tr><td><i>bypass-rest-command</i></td><td>Bypass REST command.</td></tr><tr><td><i>bypass-mode-command</i></td><td>Bypass MODE command.</td></tr></table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>oversize</i>	Block oversized file.	<i>splice</i>	Enable splice mode.	<i>bypass-rest-command</i>	Bypass REST command.	<i>bypass-mode-command</i>	Bypass MODE command.			
	Option	Description														
	<i>clientcomfort</i>	Prevent client timeout.														
	<i>oversize</i>	Block oversized file.														
	<i>splice</i>	Enable splice mode.														
	<i>bypass-rest-command</i>	Bypass REST command.														
<i>bypass-mode-command</i>	Bypass MODE command.															
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 10 1 Maximum value: 1606 **													
ports	Ports to scan for content (1 - 65535, default = 21).	integer	Minimum value: 1 Maximum value: 65535													
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no</i></td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td><i>yes</i></td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.									
	Option	Description														
	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.														
<i>yes</i>	SSL decryption and encryption performed by an external device.															
status	Enable/disable the active status of scanning for this protocol.	option	-	enable												

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions (unlimited = 0, default = 0).	integer	Minimum value: 0 0 Maximum value: 4294967295											
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 16777216	8388608										
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 16777216	262144										
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-tuning</i></td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td><i>system</i></td><td>Use system default TCP window size for this protocol.</td></tr><tr><td><i>static</i></td><td>Manually specify TCP window size.</td></tr><tr><td><i>dynamic</i></td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>	Option	Description	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).	<i>system</i>	Use system default TCP window size for this protocol.	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
	Option	Description												
	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).												
	<i>system</i>	Use system default TCP window size for this protocol.												
	<i>static</i>	Manually specify TCP window size.												
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 2 Maximum value: 100	12										
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 10 1 Maximum value: 1606 **	10										

** Values may differ between models.

config http

Parameter	Description	Type	Size	Default								
address-ip-rating	Enable/disable IP based URL rating.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
block-page-status-code	Code number returned for blocked HTTP pages (non-FortiGuard only) (100 - 599, default = 403).	integer	Minimum value: 100 Maximum value: 599	403								
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1								
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 1 Maximum value: 900	10								
domain-fronting *	Configure HTTP domain fronting (default = block).	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow domain fronting.</td></tr><tr><td><i>block</i></td><td>Block and log domain fronting.</td></tr><tr><td><i>monitor</i></td><td>Allow and log domain fronting.</td></tr></table>	Option	Description	<i>allow</i>	Allow domain fronting.	<i>block</i>	Block and log domain fronting.	<i>monitor</i>	Allow and log domain fronting.			
Option	Description											
<i>allow</i>	Allow domain fronting.											
<i>block</i>	Block and log domain fronting.											
<i>monitor</i>	Allow and log domain fronting.											
h2c	Enable/disable h2c HTTP connection upgrade.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow h2c HTTP connection upgrades. h2c tunnels do not support content scan.</td></tr><tr><td><i>disable</i></td><td>Do not allow h2c HTTP connection upgrades.</td></tr></table>	Option	Description	<i>enable</i>	Allow h2c HTTP connection upgrades. h2c tunnels do not support content scan.	<i>disable</i>	Do not allow h2c HTTP connection upgrades.					
Option	Description											
<i>enable</i>	Allow h2c HTTP connection upgrades. h2c tunnels do not support content scan.											
<i>disable</i>	Do not allow h2c HTTP connection upgrades.											
http-0.9	Configure action to take upon receipt of HTTP 0.9 request.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow HTTP 0.9 traffic for web filtering only.</td></tr><tr><td><i>block</i></td><td>Block HTTP 0.9 traffic.</td></tr></table>	Option	Description	<i>allow</i>	Allow HTTP 0.9 traffic for web filtering only.	<i>block</i>	Block HTTP 0.9 traffic.					
Option	Description											
<i>allow</i>	Allow HTTP 0.9 traffic for web filtering only.											
<i>block</i>	Block HTTP 0.9 traffic.											

Parameter	Description	Type	Size	Default																				
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
Option	Description																							
<i>enable</i>	Enable setting.																							
<i>disable</i>	Disable setting.																							
options	One or more options that can be applied to the session.	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>clientcomfort</i></td><td>Prevent client timeout.</td></tr><tr><td><i>servercomfort</i></td><td>Prevent server timeout.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file.</td></tr><tr><td><i>chunkedbypass</i></td><td>Bypass chunked transfer encoded sites.</td></tr></table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>servercomfort</i>	Prevent server timeout.	<i>oversize</i>	Block oversized file.	<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.													
Option	Description																							
<i>clientcomfort</i>	Prevent client timeout.																							
<i>servercomfort</i>	Prevent server timeout.																							
<i>oversize</i>	Block oversized file.																							
<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.																							
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 10 1 Maximum value: 1606 **																					
ports	Ports to scan for content (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535																					
post-lang	ID codes for character sets to be used to convert to UTF-8 for banned words and DLP on HTTP posts (maximum of 5 character sets).	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>jisx0201</i></td><td>Japanese Industrial Standard 0201.</td></tr><tr><td><i>jisx0208</i></td><td>Japanese Industrial Standard 0208.</td></tr><tr><td><i>jisx0212</i></td><td>Japanese Industrial Standard 0212.</td></tr><tr><td><i>gb2312</i></td><td>Guojia Biaozhun 2312 (simplified Chinese).</td></tr><tr><td><i>ksc5601-ex</i></td><td>Wansung Korean standard 5601.</td></tr><tr><td><i>euc-jp</i></td><td>Extended Unicode Japanese.</td></tr><tr><td><i>sjis</i></td><td>Shift Japanese Industrial Standard.</td></tr><tr><td><i>iso2022-jp</i></td><td>ISO 2022 Japanese.</td></tr><tr><td><i>iso2022-jp-1</i></td><td>ISO 2022-1 Japanese.</td></tr></table>	Option	Description	<i>jisx0201</i>	Japanese Industrial Standard 0201.	<i>jisx0208</i>	Japanese Industrial Standard 0208.	<i>jisx0212</i>	Japanese Industrial Standard 0212.	<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).	<i>ksc5601-ex</i>	Wansung Korean standard 5601.	<i>euc-jp</i>	Extended Unicode Japanese.	<i>sjis</i>	Shift Japanese Industrial Standard.	<i>iso2022-jp</i>	ISO 2022 Japanese.	<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.			
Option	Description																							
<i>jisx0201</i>	Japanese Industrial Standard 0201.																							
<i>jisx0208</i>	Japanese Industrial Standard 0208.																							
<i>jisx0212</i>	Japanese Industrial Standard 0212.																							
<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).																							
<i>ksc5601-ex</i>	Wansung Korean standard 5601.																							
<i>euc-jp</i>	Extended Unicode Japanese.																							
<i>sjis</i>	Shift Japanese Industrial Standard.																							
<i>iso2022-jp</i>	ISO 2022 Japanese.																							
<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.																							

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>iso2022-jp-2</i></td><td>ISO 2022-2 Japanese.</td></tr><tr><td><i>euc-cn</i></td><td>Extended Unicode Chinese.</td></tr><tr><td><i>ces-gbk</i></td><td>Extended GB2312 (simplified Chinese).</td></tr><tr><td><i>hz</i></td><td>Hanzi simplified Chinese.</td></tr><tr><td><i>ces-big5</i></td><td>Big-5 traditional Chinese.</td></tr><tr><td><i>euc-kr</i></td><td>Extended Unicode Korean.</td></tr><tr><td><i>iso2022-jp-3</i></td><td>ISO 2022-3 Japanese.</td></tr><tr><td><i>iso8859-1</i></td><td>ISO 8859 Part 1 (Western European).</td></tr><tr><td><i>tis620</i></td><td>Thai Industrial Standard 620.</td></tr><tr><td><i>cp874</i></td><td>Code Page 874 (Thai).</td></tr><tr><td><i>cp1252</i></td><td>Code Page 1252 (Western European Latin).</td></tr><tr><td><i>cp1251</i></td><td>Code Page 1251 (Cyrillic).</td></tr></table>	Option	Description	<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.	<i>euc-cn</i>	Extended Unicode Chinese.	<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).	<i>hz</i>	Hanzi simplified Chinese.	<i>ces-big5</i>	Big-5 traditional Chinese.	<i>euc-kr</i>	Extended Unicode Korean.	<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.	<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).	<i>tis620</i>	Thai Industrial Standard 620.	<i>cp874</i>	Code Page 874 (Thai).	<i>cp1252</i>	Code Page 1252 (Western European Latin).	<i>cp1251</i>	Code Page 1251 (Cyrillic).			
	Option	Description																												
	<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.																												
	<i>euc-cn</i>	Extended Unicode Chinese.																												
	<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).																												
	<i>hz</i>	Hanzi simplified Chinese.																												
	<i>ces-big5</i>	Big-5 traditional Chinese.																												
	<i>euc-kr</i>	Extended Unicode Korean.																												
	<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.																												
	<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).																												
	<i>tis620</i>	Thai Industrial Standard 620.																												
	<i>cp874</i>	Code Page 874 (Thai).																												
	<i>cp1252</i>	Code Page 1252 (Western European Latin).																												
<i>cp1251</i>	Code Page 1251 (Cyrillic).																													
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																							
	Option	Description																												
	<i>enable</i>	Enable setting.																												
<i>disable</i>	Disable setting.																													
range-block	Enable/disable blocking of partial downloads.	option	-	disable																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable range header blocking (allow partial file downloads)</td></tr><tr><td><i>enable</i></td><td>Enable range header blocking (treat all partial file downloads as full file download)</td></tr></table>	Option	Description	<i>disable</i>	Disable range header blocking (allow partial file downloads)	<i>enable</i>	Enable range header blocking (treat all partial file downloads as full file download)																							
	Option	Description																												
	<i>disable</i>	Disable range header blocking (allow partial file downloads)																												
<i>enable</i>	Enable range header blocking (treat all partial file downloads as full file download)																													
retry-count	Number of attempts to retry HTTP connection (0 - 100, default = 0).	integer	Minimum value: 0 0 Maximum value: 100																											
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable																										

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no</i></td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td><i>yes</i></td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
	Option	Description								
	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.								
<i>yes</i>	SSL decryption and encryption performed by an external device.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions (unlimited = 0, default = 0).	integer	Minimum value: 0 0 Maximum value: 4294967295							
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable bypassing of streaming content from buffering</td></tr><tr><td><i>disable</i></td><td>Disable bypassing of streaming content from buffering</td></tr></table>	Option	Description	<i>enable</i>	Enable bypassing of streaming content from buffering	<i>disable</i>	Disable bypassing of streaming content from buffering			
	Option	Description								
	<i>enable</i>	Enable bypassing of streaming content from buffering								
<i>disable</i>	Disable bypassing of streaming content from buffering									
strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable changing of HTTP X-Forwarded-For header.</td></tr><tr><td><i>enable</i></td><td>Enable replacement of X-Forwarded-For value with 1.1.1.1.</td></tr></table>	Option	Description	<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.	<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.			
	Option	Description								
	<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.								
<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.									
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-	bypass						

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass connections when switching protocols.</td></tr><tr><td>block</td><td>Block connections when switching protocols.</td></tr></table>	Option	Description	bypass	Bypass connections when switching protocols.	block	Block connections when switching protocols.							
	Option	Description												
	bypass	Bypass connections when switching protocols.												
block	Block connections when switching protocols.													
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 16777216	8388608										
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 16777216	262144										
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto-tuning</td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td>system</td><td>Use system default TCP window size for this protocol.</td></tr><tr><td>static</td><td>Manually specify TCP window size.</td></tr><tr><td>dynamic</td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>	Option	Description	auto-tuning	Allow system to auto-tune TCP window size (default).	system	Use system default TCP window size for this protocol.	static	Manually specify TCP window size.	dynamic	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
	Option	Description												
	auto-tuning	Allow system to auto-tune TCP window size (default).												
	system	Use system default TCP window size for this protocol.												
	static	Manually specify TCP window size.												
dynamic	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
tunnel-non-http	Configure how to process non-HTTP traffic when a profile configured for HTTP traffic accepts a non-HTTP session. Can occur if an application sends non-HTTP traffic using an HTTP destination port.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td></tr><tr><td>disable</td><td>Drop or tear down non-HTTP sessions accepted by the profile.</td></tr></table>	Option	Description	enable	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	disable	Drop or tear down non-HTTP sessions accepted by the profile.							
	Option	Description												
	enable	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.												
disable	Drop or tear down non-HTTP sessions accepted by the profile.													

Parameter	Description	Type	Size	Default								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100	12								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10								
unknown-content-encoding	Configure the action the FortiGate unit will take on unknown content-encoding.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block HTTP session when unknown content-encoding is detected.</td></tr><tr><td><i>inspect</i></td><td>Scan HTTP traffic as plain-text when unknown content-encoding is detected.</td></tr><tr><td><i>bypass</i></td><td>Bypass scan when unknown content-encoding is detected.</td></tr></table>	Option	Description	<i>block</i>	Block HTTP session when unknown content-encoding is detected.	<i>inspect</i>	Scan HTTP traffic as plain-text when unknown content-encoding is detected.	<i>bypass</i>	Bypass scan when unknown content-encoding is detected.			
Option	Description											
<i>block</i>	Block HTTP session when unknown content-encoding is detected.											
<i>inspect</i>	Scan HTTP traffic as plain-text when unknown content-encoding is detected.											
<i>bypass</i>	Bypass scan when unknown content-encoding is detected.											
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reject</i></td><td>Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.</td></tr><tr><td><i>tunnel</i></td><td>Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td></tr><tr><td><i>best-effort</i></td><td>Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.</td></tr></table>	Option	Description	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.	<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.			
Option	Description											
<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.											
<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.											
<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.											
verify-dns-for-policy-matching	Enable/disable verification of DNS for policy matching.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

* This parameter may not exist in some models.

** Values may differ between models.

config imap

Parameter	Description	Type	Size	Default						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized email.</td></tr></table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized email.									
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10						
ports	Ports to scan for content (1 - 65535, default = 143).	integer	Minimum value: 1 Maximum value: 65535							
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no</td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td>yes</td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	yes	SSL decryption and encryption performed by an external device.			
	Option	Description								
	no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.								
yes	SSL decryption and encryption performed by an external device.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100	12						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10						

** Values may differ between models.

config mail-signature

Parameter	Description	Type	Size	Default						
signature	Email signature to be added to outgoing email (if the signature contains spaces, enclose with quotation marks).	string	Maximum length: 1023							
status	Enable/disable adding an email signature to SMTP email messages as they pass through the FortiGate.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable mail signature.</td></tr><tr><td>enable</td><td>Enable mail signature.</td></tr></table>				Option	Description	disable	Disable mail signature.	enable	Enable mail signature.
Option	Description									
disable	Disable mail signature.									
enable	Enable mail signature.									

config mapi

Parameter	Description	Type	Size	Default						
options	One or more options that can be applied to the session.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized email.</td></tr></table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized email.									
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10						
ports	Ports to scan for content (1 - 65535, default = 135).	integer	Minimum value: 1 Maximum value: 65535							
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100	12						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10						

** Values may differ between models.

config nntp

Parameter	Description	Type	Size	Default						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>oversize</i></td><td>Block oversized file.</td></tr><tr><td><i>splice</i></td><td>Enable splice mode.</td></tr></table>	Option	Description	<i>oversize</i>	Block oversized file.	<i>splice</i>	Enable splice mode.			
Option	Description									
<i>oversize</i>	Block oversized file.									
<i>splice</i>	Enable splice mode.									
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10						
ports	Ports to scan for content (1 - 65535, default = 119).	integer	Minimum value: 1 Maximum value: 65535							
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>			Enable setting.
	<i>disable</i>			Disable setting.
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10

** Values may differ between models.

config pop3

Parameter	Description	Type	Size	Default
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
	Option Description			
	<i>enable</i>			Enable setting.
	<i>disable</i>			Disable setting.
options	One or more options that can be applied to the session.	option	-	
	Option Description			
	<i>fragmail</i>			Pass fragmented email.
	<i>oversize</i>			Block oversized email.
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content (1 - 65535, default = 110).	integer	Minimum value: 1 Maximum value: 65535							
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no</td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td>yes</td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	yes	SSL decryption and encryption performed by an external device.			
Option	Description									
no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.									
yes	SSL decryption and encryption performed by an external device.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100	12						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10						

** Values may differ between models.

config smtp

Parameter	Description	Type	Size	Default
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	Option	Description		
	<i>fragmail</i>	Pass fragmented email.		
	<i>oversize</i>	Block oversized email.		
	<i>splice</i>	Enable splice mode.		
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10
ports	Ports to scan for content (1 - 65535, default = 25).	integer	Minimum value: 1 Maximum value: 65535	
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
server-busy	Enable/disable SMTP server busy when server not available.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no</i></td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td><i>yes</i></td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.			
Option	Description									
<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100	12						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10						

** Values may differ between models.

config ssh

Parameter	Description	Type	Size	Default
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1

Parameter	Description	Type	Size	Default								
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 10 1 Maximum value: 900									
options	One or more options that can be applied to the session.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>oversize</td><td>Block oversized file.</td></tr><tr><td>clientcomfort</td><td>Prevent client timeout.</td></tr><tr><td>servercomfort</td><td>Prevent server timeout.</td></tr></table>	Option	Description	oversize	Block oversized file.	clientcomfort	Prevent client timeout.	servercomfort	Prevent server timeout.			
Option	Description											
oversize	Block oversized file.											
clientcomfort	Prevent client timeout.											
servercomfort	Prevent server timeout.											
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 10 1 Maximum value: 1606 **									
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
Option	Description											
enable	Enable setting.											
disable	Disable setting.											
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no</td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td>yes</td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	yes	SSL decryption and encryption performed by an external device.					
Option	Description											
no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.											
yes	SSL decryption and encryption performed by an external device.											
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions (unlimited = 0, default = 0).	integer	Minimum value: 0 0 Maximum value: 4294967295									
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 8388608 1048576 Maximum value: 16777216									

Parameter	Description	Type	Size	Default
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 16777216	262144
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning
	Option		Description	
	<i>auto-tuning</i>		Allow system to auto-tune TCP window size (default).	
	<i>system</i>		Use system default TCP window size for this protocol.	
	<i>static</i>		Manually specify TCP window size.	
	<i>dynamic</i>		Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.	
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 1606 **	10

** Values may differ between models.

config firewall proxy-address

Configure web proxy address.

```

config firewall proxy-address
  Description: Configure web proxy address.
  edit <name>
    set application <name1>, <name2>, ...
    set case-sensitivity [disable|enable]
    set category <id1>, <id2>, ...
    set color {integer}
    set comment {var-string}
    set header {string}
    config header-group
      Description: HTTP header group.

```

```

        edit <id>
            set case-sensitivity [disable|enable]
            set header {string}
            set header-name {string}
        next
    end
    set header-name {string}
    set host {string}
    set host-regex {string}
    set method {option1}, {option2}, ...
    set path {string}
    set query {string}
    set referrer [enable|disable]
    config tagging
        Description: Config object tagging.
        edit <name>
            set category {string}
            set tags <name1>, <name2>, ...
        next
    end
    set type [host-regex|url|...]
    set ua {option1}, {option2}, ...
    set ua-max-ver {string}
    set ua-min-ver {string}
    set uuid {uuid}
next
end

```

config firewall proxy-address

Parameter	Description	Type	Size	Default
application <name>	SaaS application. SaaS application name.	string	Maximum length: 79	
case- sensitivity	Enable to make the pattern case sensitive.	option	-	disable
	Option	Description		
	disable	Case insensitive in pattern.		
	enable	Case sensitive in pattern.		
category <id>	FortiGuard category ID. FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default																								
color	Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1).	integer	Minimum value: 0 Maximum value: 32																									
comment	Optional comments.	var-string	Maximum length: 255																									
header	HTTP header name as a regular expression.	string	Maximum length: 255																									
header-name	Name of HTTP header.	string	Maximum length: 79																									
host	Address object for the host.	string	Maximum length: 79																									
host-regex	Host name as a regular expression.	string	Maximum length: 255																									
method	HTTP request methods to be used.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>get</i></td><td>GET method.</td></tr><tr><td><i>post</i></td><td>POST method.</td></tr><tr><td><i>put</i></td><td>PUT method.</td></tr><tr><td><i>head</i></td><td>HEAD method.</td></tr><tr><td><i>connect</i></td><td>CONNECT method.</td></tr><tr><td><i>trace</i></td><td>TRACE method.</td></tr><tr><td><i>options</i></td><td>OPTIONS method.</td></tr><tr><td><i>delete</i></td><td>DELETE method.</td></tr><tr><td><i>update</i></td><td>UPDATE method.</td></tr><tr><td><i>patch</i></td><td>PATCH method.</td></tr><tr><td><i>other</i></td><td>Other methods.</td></tr></table>				Option	Description	<i>get</i>	GET method.	<i>post</i>	POST method.	<i>put</i>	PUT method.	<i>head</i>	HEAD method.	<i>connect</i>	CONNECT method.	<i>trace</i>	TRACE method.	<i>options</i>	OPTIONS method.	<i>delete</i>	DELETE method.	<i>update</i>	UPDATE method.	<i>patch</i>	PATCH method.	<i>other</i>	Other methods.
Option	Description																											
<i>get</i>	GET method.																											
<i>post</i>	POST method.																											
<i>put</i>	PUT method.																											
<i>head</i>	HEAD method.																											
<i>connect</i>	CONNECT method.																											
<i>trace</i>	TRACE method.																											
<i>options</i>	OPTIONS method.																											
<i>delete</i>	DELETE method.																											
<i>update</i>	UPDATE method.																											
<i>patch</i>	PATCH method.																											
<i>other</i>	Other methods.																											
name	Address name.	string	Maximum length: 79																									
path	URL path as a regular expression.	string	Maximum length: 255																									
query	Match the query part of the URL as a regular expression.	string	Maximum length: 255																									
referrer	Enable/disable use of referrer field in the HTTP header to match the address.	option	-	disable																								

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
	Option	Description																						
	<i>enable</i>	Enable setting.																						
<i>disable</i>	Disable setting.																							
type	Proxy address type.	option	-	url																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>host-regex</i></td><td>Host regular expression.</td></tr><tr><td><i>url</i></td><td>HTTP URL.</td></tr><tr><td><i>category</i></td><td>FortiGuard URL catgegory.</td></tr><tr><td><i>method</i></td><td>HTTP request method.</td></tr><tr><td><i>ua</i></td><td>HTTP request user agent.</td></tr><tr><td><i>header</i></td><td>HTTP request header.</td></tr><tr><td><i>src-advanced</i></td><td>HTTP advanced source criteria.</td></tr><tr><td><i>dst-advanced</i></td><td>HTTP advanced destination criteria.</td></tr><tr><td><i>saas</i></td><td>SaaS application.</td></tr></table>	Option	Description	<i>host-regex</i>	Host regular expression.	<i>url</i>	HTTP URL.	<i>category</i>	FortiGuard URL catgegory.	<i>method</i>	HTTP request method.	<i>ua</i>	HTTP request user agent.	<i>header</i>	HTTP request header.	<i>src-advanced</i>	HTTP advanced source criteria.	<i>dst-advanced</i>	HTTP advanced destination criteria.	<i>saas</i>	SaaS application.			
	Option	Description																						
	<i>host-regex</i>	Host regular expression.																						
	<i>url</i>	HTTP URL.																						
	<i>category</i>	FortiGuard URL catgegory.																						
	<i>method</i>	HTTP request method.																						
	<i>ua</i>	HTTP request user agent.																						
	<i>header</i>	HTTP request header.																						
	<i>src-advanced</i>	HTTP advanced source criteria.																						
<i>dst-advanced</i>	HTTP advanced destination criteria.																							
<i>saas</i>	SaaS application.																							
ua	Names of browsers to be used as user agent.	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chrome</i></td><td>Google Chrome.</td></tr><tr><td><i>ms</i></td><td>Microsoft Internet Explorer or EDGE.</td></tr><tr><td><i>firefox</i></td><td>Mozilla Firefox.</td></tr><tr><td><i>safari</i></td><td>Apple Safari.</td></tr><tr><td><i>ie</i></td><td>Microsoft Internet Explorer.</td></tr><tr><td><i>edge</i></td><td>Microsoft Edge.</td></tr><tr><td><i>other</i></td><td>Other browsers.</td></tr></table>	Option	Description	<i>chrome</i>	Google Chrome.	<i>ms</i>	Microsoft Internet Explorer or EDGE.	<i>firefox</i>	Mozilla Firefox.	<i>safari</i>	Apple Safari.	<i>ie</i>	Microsoft Internet Explorer.	<i>edge</i>	Microsoft Edge.	<i>other</i>	Other browsers.							
	Option	Description																						
	<i>chrome</i>	Google Chrome.																						
	<i>ms</i>	Microsoft Internet Explorer or EDGE.																						
	<i>firefox</i>	Mozilla Firefox.																						
	<i>safari</i>	Apple Safari.																						
	<i>ie</i>	Microsoft Internet Explorer.																						
<i>edge</i>	Microsoft Edge.																							
<i>other</i>	Other browsers.																							
ua-max-ver	Maximum version of the user agent specified in dotted notation. For example, use 120 with the ua field set to "chrome" to require Google Chrome's maximum version must be 120.	string	Maximum length: 63																					

Parameter	Description	Type	Size	Default
ua-min-ver	Minimum version of the user agent specified in dotted notation. For example, use 90.0.1 with the ua field set to "chrome" to require Google Chrome's minimum version must be 90.0.1.	string	Maximum length: 63	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config header-group

Parameter	Description	Type	Size	Default						
case-sensitivity	Case sensitivity in pattern.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Case insensitive in pattern.</td></tr><tr><td><i>enable</i></td><td>Case sensitive in pattern.</td></tr></table>	Option	Description	<i>disable</i>	Case insensitive in pattern.	<i>enable</i>	Case sensitive in pattern.			
Option	Description									
<i>disable</i>	Case insensitive in pattern.									
<i>enable</i>	Case sensitive in pattern.									
header	HTTP header regular expression.	string	Maximum length: 255							
header-name	HTTP header.	string	Maximum length: 79							
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall proxy-addrgrp

Configure web proxy address group.

```
config firewall proxy-addrgrp
  Description: Configure web proxy address group.
  edit <name>
    set color {integer}
    set comment {var-string}
    set member <name1>, <name2>, ...
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set type [src|dst]
    set uuid {uuid}
  next
end
```

config firewall proxy-addrgrp

Parameter	Description	Type	Size	Default
color	Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1).	integer	Minimum value: 0 Maximum value: 32	0
comment	Optional comments.	var-string	Maximum length: 255	
member <name>	Members of address group. Address name.	string	Maximum length: 79	
name	Address group name.	string	Maximum length: 79	
type	Source or destination address group type.	option	-	src
		Option	Description	
		src	Source group.	
		dst	Destination group.	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall proxy-policy

Configure proxy policies.

```
config firewall proxy-policy
  Description: Configure proxy policies.
  edit <policyid>
    set access-proxy <name1>, <name2>, ...
    set access-proxy6 <name1>, <name2>, ...
    set action [accept|deny|...]
    set application-list {string}
    set av-profile {string}
    set block-notification [enable|disable]
    set casb-profile {string}
    set comments {var-string}
    set decrypted-traffic-mirror {string}
    set detect-https-in-http-request [enable|disable]
    set device-ownership [enable|disable]
    set disclaimer [disable|domain|...]
    set dlp-profile {string}
    set dnsfilter-profile {string}
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set dstaddr6 <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set emailfilter-profile {string}
    set file-filter-profile {string}
    set groups <name1>, <name2>, ...
    set http-tunnel-auth [enable|disable]
    set https-sub-category [enable|disable]
    set icap-profile {string}
    set internet-service [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-name <name1>, <name2>, ...
    set internet-service-negate [enable|disable]
```

```

set internet-service6 [enable|disable]
set internet-service6-custom <name1>, <name2>, ...
set internet-service6-custom-group <name1>, <name2>, ...
set internet-service6-group <name1>, <name2>, ...
set internet-service6-name <name1>, <name2>, ...
set internet-service6-negate [enable|disable]
set ips-sensor {string}
set ips-voip-filter {string}
set isolator-server {string}
set log-http-transaction [enable|disable]
set logtraffic [all|utm|...]
set logtraffic-start [enable|disable]
set name {string}
set poolname <name1>, <name2>, ...
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set proxy [explicit-web|transparent-web|...]
set redirect-url {var-string}
set replacemsg-override-group {string}
set schedule {string}
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set session-ttl {integer}
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcaddr6 <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssh-policy-redirect [enable|disable]
set ssl-ssh-profile {string}
set status [enable|disable]
set telemetry-profile {string}
set transparent [enable|disable]
set url-risk <name1>, <name2>, ...
set users <name1>, <name2>, ...
set utm-status [enable|disable]
set uuid {uuid}
set videofilter-profile {string}
set waf-profile {string}
set webcache [enable|disable]
set webcache-https [disable|enable]
set webfilter-profile {string}
set webproxy-forward-server {string}
set webproxy-profile {string}
set ztna-ems-tag <name1>, <name2>, ...
set ztna-ems-tag-negate [enable|disable]
set ztna-proxy <name1>, <name2>, ...
set ztna-tags-match-logic [or|and]
next
end

```


config firewall proxy-policy

Parameter	Description	Type	Size	Default										
access-proxy <name>	IPv4 access proxy. Access Proxy name.	string	Maximum length: 79											
access-proxy6 <name>	IPv6 access proxy. Access proxy name.	string	Maximum length: 79											
action	Accept or deny traffic matching the policy parameters.	option	-	deny										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Action accept.</td></tr><tr><td><i>deny</i></td><td>Action deny.</td></tr><tr><td><i>redirect</i></td><td>Action redirect.</td></tr><tr><td><i>isolate</i></td><td>Action isolate.</td></tr></table>	Option	Description	<i>accept</i>	Action accept.	<i>deny</i>	Action deny.	<i>redirect</i>	Action redirect.	<i>isolate</i>	Action isolate.			
Option	Description													
<i>accept</i>	Action accept.													
<i>deny</i>	Action deny.													
<i>redirect</i>	Action redirect.													
<i>isolate</i>	Action isolate.													
application-list	Name of an existing Application list.	string	Maximum length: 47											
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 47											
block- notification	Enable/disable block notification.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
casb-profile	Name of an existing CASB profile.	string	Maximum length: 47											
comments	Optional comments.	var-string	Maximum length: 1023											
decrypted- traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35											
detect-https- in-http- request	Enable/disable detection of HTTPS in HTTP request.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable detection of HTTPS in HTTP request.</td></tr><tr><td><i>disable</i></td><td>Disable detection of HTTPS in HTTP request.</td></tr></table>	Option	Description	<i>enable</i>	Enable detection of HTTPS in HTTP request.	<i>disable</i>	Disable detection of HTTPS in HTTP request.							
Option	Description													
<i>enable</i>	Enable detection of HTTPS in HTTP request.													
<i>disable</i>	Disable detection of HTTPS in HTTP request.													

Parameter	Description	Type	Size	Default										
device-ownership	When enabled, the ownership enforcement will be done at policy level.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable device ownership.</td></tr><tr><td><i>disable</i></td><td>Disable device ownership.</td></tr></table>	Option	Description	<i>enable</i>	Enable device ownership.	<i>disable</i>	Disable device ownership.							
	Option	Description												
	<i>enable</i>	Enable device ownership.												
<i>disable</i>	Disable device ownership.													
disclaimer	Web proxy disclaimer setting: by domain, policy, or user.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable disclaimer.</td></tr><tr><td><i>domain</i></td><td>Display disclaimer for domain</td></tr><tr><td><i>policy</i></td><td>Display disclaimer for policy</td></tr><tr><td><i>user</i></td><td>Display disclaimer for current user</td></tr></table>	Option	Description	<i>disable</i>	Disable disclaimer.	<i>domain</i>	Display disclaimer for domain	<i>policy</i>	Display disclaimer for policy	<i>user</i>	Display disclaimer for current user			
	Option	Description												
	<i>disable</i>	Disable disclaimer.												
	<i>domain</i>	Display disclaimer for domain												
	<i>policy</i>	Display disclaimer for policy												
<i>user</i>	Display disclaimer for current user													
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 47											
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 47											
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79											
dstaddr-negate	When enabled, destination addresses match against any address EXCEPT the specified destination addresses.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negate.</td></tr><tr><td><i>disable</i></td><td>Disable destination address negate.</td></tr></table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable destination address negate.							
	Option	Description												
	<i>enable</i>	Enable source address negate.												
<i>disable</i>	Disable destination address negate.													
dstaddr6 <name>	IPv6 destination address objects. Address name.	string	Maximum length: 79											
dstintf <name>	Destination interface names. Interface name.	string	Maximum length: 79											
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 47											
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 47											

Parameter	Description	Type	Size	Default						
groups <name>	Names of group objects. Group name.	string	Maximum length: 79							
http-tunnel-auth	Enable/disable HTTP tunnel authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
https-sub-category	Enable/disable HTTPS sub-category policy matching.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTPS sub-category policy matching.</td></tr><tr><td><i>disable</i></td><td>Disable HTTPS sub-category policy matching.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTPS sub-category policy matching.	<i>disable</i>	Disable HTTPS sub-category policy matching.			
Option	Description									
<i>enable</i>	Enable HTTPS sub-category policy matching.									
<i>disable</i>	Disable HTTPS sub-category policy matching.									
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 47							
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Services in policy.									
<i>disable</i>	Disable use of Internet Services in policy.									
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
internet-service-negate	When enabled, Internet Services match against any internet service EXCEPT the selected Internet Service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated Internet Service match.</td></tr><tr><td>disable</td><td>Disable negated Internet Service match.</td></tr></table>	Option	Description	enable	Enable negated Internet Service match.	disable	Disable negated Internet Service match.			
Option	Description									
enable	Enable negated Internet Service match.									
disable	Disable negated Internet Service match.									
internet-service6	Enable/disable use of Internet Services IPv6 for this policy. If enabled, destination IPv6 address and service are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of IPv6 Internet Services in policy.</td></tr><tr><td>disable</td><td>Disable use of IPv6 Internet Services in policy.</td></tr></table>	Option	Description	enable	Enable use of IPv6 Internet Services in policy.	disable	Disable use of IPv6 Internet Services in policy.			
Option	Description									
enable	Enable use of IPv6 Internet Services in policy.									
disable	Disable use of IPv6 Internet Services in policy.									
internet-service6-custom <name>	Custom Internet Service IPv6 name. Custom Internet Service IPv6 name.	string	Maximum length: 79							
internet-service6-custom-group <name>	Custom Internet Service IPv6 group name. Custom Internet Service IPv6 group name.	string	Maximum length: 79							
internet-service6-group <name>	Internet Service IPv6 group name. Internet Service IPv6 group name.	string	Maximum length: 79							
internet-service6-name <name>	Internet Service IPv6 name. Internet Service IPv6 name.	string	Maximum length: 79							
internet-service6-negate	When enabled, Internet Services match against any internet service IPv6 EXCEPT the selected Internet Service IPv6.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated IPv6 Internet Service match.</td></tr><tr><td>disable</td><td>Disable negated IPv6 Internet Service match.</td></tr></table>	Option	Description	enable	Enable negated IPv6 Internet Service match.	disable	Disable negated IPv6 Internet Service match.			
Option	Description									
enable	Enable negated IPv6 Internet Service match.									
disable	Disable negated IPv6 Internet Service match.									
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 47							

Parameter	Description	Type	Size	Default								
ips-voip-filter	Name of an existing VoIP (ips) profile.	string	Maximum length: 47									
isolator-server	Isolator server name.	string	Maximum length: 63									
log-http-transaction	Enable/disable HTTP transaction log.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP transaction log.</td></tr><tr><td>disable</td><td>Disable HTTP transaction log.</td></tr></table>	Option	Description	enable	Enable HTTP transaction log.	disable	Disable HTTP transaction log.					
Option	Description											
enable	Enable HTTP transaction log.											
disable	Disable HTTP transaction log.											
logtraffic	Enable/disable logging traffic through the policy.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Log all sessions.</td></tr><tr><td>utm</td><td>UTM event and matched application traffic log.</td></tr><tr><td>disable</td><td>Disable traffic and application log.</td></tr></table>	Option	Description	all	Log all sessions.	utm	UTM event and matched application traffic log.	disable	Disable traffic and application log.			
Option	Description											
all	Log all sessions.											
utm	UTM event and matched application traffic log.											
disable	Disable traffic and application log.											
logtraffic-start	Enable/disable policy log traffic start.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
Option	Description											
enable	Enable setting.											
disable	Disable setting.											
name	Policy name.	string	Maximum length: 35									
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295									
poolname <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79									
profile-group	Name of profile group.	string	Maximum length: 47									
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 47	default								

Parameter	Description	Type	Size	Default																		
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>single</td><td>Do not allow security profile groups.</td></tr><tr><td>group</td><td>Allow security profile groups.</td></tr></table>	Option	Description	single	Do not allow security profile groups.	group	Allow security profile groups.															
Option	Description																					
single	Do not allow security profile groups.																					
group	Allow security profile groups.																					
proxy	Type of explicit proxy.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>explicit-web</td><td>Explicit Web Proxy</td></tr><tr><td>transparent-web</td><td>Transparent Web Proxy</td></tr><tr><td>ftp</td><td>Explicit FTP Proxy</td></tr><tr><td>ssh</td><td>SSH Proxy</td></tr><tr><td>ssh-tunnel</td><td>SSH Tunnel</td></tr><tr><td>access-proxy</td><td>Access Proxy</td></tr><tr><td>ztna-proxy</td><td>ZTNA Proxy</td></tr><tr><td>wanopt</td><td>WANopt Tunnel</td></tr></table>	Option	Description	explicit-web	Explicit Web Proxy	transparent-web	Transparent Web Proxy	ftp	Explicit FTP Proxy	ssh	SSH Proxy	ssh-tunnel	SSH Tunnel	access-proxy	Access Proxy	ztna-proxy	ZTNA Proxy	wanopt	WANopt Tunnel			
Option	Description																					
explicit-web	Explicit Web Proxy																					
transparent-web	Transparent Web Proxy																					
ftp	Explicit FTP Proxy																					
ssh	SSH Proxy																					
ssh-tunnel	SSH Tunnel																					
access-proxy	Access Proxy																					
ztna-proxy	ZTNA Proxy																					
wanopt	WANopt Tunnel																					
redirect-url	Redirect URL for further explicit web proxy processing.	var-string	Maximum length: 1023																			
replacemsg-override-group	Authentication replacement message override group.	string	Maximum length: 35																			
schedule	Name of schedule object.	string	Maximum length: 35																			
service <name>	Name of service objects. Service name.	string	Maximum length: 79																			
service-negate	When enabled, services match against any service EXCEPT the specified destination services.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated service match.</td></tr><tr><td>disable</td><td>Disable negated service match.</td></tr></table>	Option	Description	enable	Enable negated service match.	disable	Disable negated service match.															
Option	Description																					
enable	Enable negated service match.																					
disable	Disable negated service match.																					

Parameter	Description	Type	Size	Default						
session-ttl	TTL in seconds for sessions accepted by this policy (0 means use the system default session TTL).	integer	Minimum value: 0 300 Maximum value: 2764800							
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled, source addresses match against any address EXCEPT the specified source addresses.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source address negate.</td></tr><tr><td>disable</td><td>Disable destination address negate.</td></tr></table>	Option	Description	enable	Enable source address negate.	disable	Disable destination address negate.			
Option	Description									
enable	Enable source address negate.									
disable	Disable destination address negate.									
srcaddr6 <name>	IPv6 source address objects. Address name.	string	Maximum length: 79							
srcintf <name>	Source interface names. Interface name.	string	Maximum length: 79							
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 47							
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SSH policy redirect.</td></tr><tr><td>disable</td><td>Disable SSH policy redirect.</td></tr></table>	Option	Description	enable	Enable SSH policy redirect.	disable	Disable SSH policy redirect.			
Option	Description									
enable	Enable SSH policy redirect.									
disable	Disable SSH policy redirect.									
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 47	no-inspection						
status	Enable/disable the active status of the policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
telemetry-profile *	Name of an existing telemetry profile.	string	Maximum length: 47							

Parameter	Description	Type	Size	Default
transparent	Enable to use the IP address of the client to connect to the server.	option	-	disable
	Option Description			
	<i>enable</i>	Enable use of IP address of client to connect to server.		
	<i>disable</i>	Disable use of IP address of client to connect to server.		
url-risk <name>	URL risk level name. Risk level name.	string	Maximum length: 79	
users <name>	Names of user objects. Group name.	string	Maximum length: 79	
utm-status	Enable the use of UTM profiles/sensors/lists.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 47	
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 47	
webcache *	Enable/disable web caching.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
webcache-https *	Enable/disable web caching for HTTPS (Requires deep-inspection enabled in ssl-ssh-profile).	option	-	disable
	Option Description			
	<i>disable</i>	Disable web cache for HTTPS.		
	<i>enable</i>	Enable web cache for HTTPS.		

Parameter	Description	Type	Size	Default						
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 47							
webproxy-forward-server	Web proxy forward server name.	string	Maximum length: 63							
webproxy-profile	Name of web proxy profile.	string	Maximum length: 63							
ztna-ems-tag <name>	ZTNA EMS Tag names. EMS Tag name.	string	Maximum length: 79							
ztna-ems-tag-negate	When enabled, ZTNA EMS tags match against any tag EXCEPT the specified ZTNA EMS tags.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ZTNA EMS tags negate.</td></tr><tr><td>disable</td><td>Disable ZTNA EMS tags negate.</td></tr></table>				Option	Description	enable	Enable ZTNA EMS tags negate.	disable	Disable ZTNA EMS tags negate.
Option	Description									
enable	Enable ZTNA EMS tags negate.									
disable	Disable ZTNA EMS tags negate.									
ztna-proxy <name>	ZTNA proxies. ZTNA proxy name.	string	Maximum length: 79							
ztna-tags-match-logic	ZTNA tag matching logic.	option	-	or						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>or</td><td>Match ZTNA tags using a logical OR operator.</td></tr><tr><td>and</td><td>Match ZTNA tags using a logical AND operator.</td></tr></table>				Option	Description	or	Match ZTNA tags using a logical OR operator.	and	Match ZTNA tags using a logical AND operator.
Option	Description									
or	Match ZTNA tags using a logical OR operator.									
and	Match ZTNA tags using a logical AND operator.									

* This parameter may not exist in some models.

config firewall region

Define region table. Read-only.

```
config firewall region
  Description: Define region table. Read-only.
  edit <id>
    set city <id1>, <id2>, ...
    set name {string}
  next
end
```

config firewall region

Parameter	Description	Type	Size	Default
city <id>	City ID list. City ID.	integer	Minimum value: 0 Maximum value: 65535	
id	Region ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	Region name.	string	Maximum length: 63	

config firewall schedule group

Schedule group configuration.

```
config firewall schedule group
  Description: Schedule group configuration.
  edit <name>
    set color {integer}
    set fabric-object [enable|disable]
    set member <name1>, <name2>, ...
    set uuid {uuid}
  next
end
```

config firewall schedule group

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable
		Option	Description	
		enable	Object is set as a security fabric-wide global object.	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Object is local to this security fabric member.		
member <name>	Schedules added to the schedule group. Schedule name.	string	Maximum length: 79	
name	Schedule group name.	string	Maximum length: 31	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000- 0000-0000- 000000000000

config firewall schedule onetime

Onetime schedule configuration.

```
config firewall schedule onetime
  Description: Onetime schedule configuration.
  edit <name>
    set color {integer}
    set end {user}
    set end-utc {user}
    set expiration-days {integer}
    set fabric-object [enable|disable]
    set start {user}
    set start-utc {user}
    set uuid {uuid}
  next
end
```

config firewall schedule onetime

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
end-utc	Schedule end date and time, in epoch format.	user	Not Specified	

Parameter	Description	Type	Size	Default						
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100	3						
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									
name	Onetime schedule name.	string	Maximum length: 31							
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified							
start-utc	Schedule start date and time, in epoch format.	user	Not Specified							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

config firewall schedule recurring

Recurring schedule configuration.

```

config firewall schedule recurring
    Description: Recurring schedule configuration.
    edit <name>
        set color {integer}
        set day {option1}, {option2}, ...
        set end {user}
        set fabric-object [enable|disable]
        set start {user}
        set uuid {uuid}
    next
end

```

config firewall schedule recurring

Parameter	Description	Type	Size	Default																		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0																		
day	One or more days of the week on which the schedule is valid. Separate the names of the days with a space.	option	-	none																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday.</td></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr><tr><td><i>none</i></td><td>None.</td></tr></table>				Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.	<i>none</i>	None.
	Option	Description																				
	<i>sunday</i>	Sunday.																				
	<i>monday</i>	Monday.																				
	<i>tuesday</i>	Tuesday.																				
	<i>wednesday</i>	Wednesday.																				
	<i>thursday</i>	Thursday.																				
	<i>friday</i>	Friday.																				
	<i>saturday</i>	Saturday.																				
<i>none</i>	None.																					
end	Time of day to end the schedule, format hh:mm.	user	Not Specified																			
fabric-object	Security Fabric global object setting.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.												
	Option	Description																				
	<i>enable</i>	Object is set as a security fabric-wide global object.																				
<i>disable</i>	Object is local to this security fabric member.																					
name	Recurring schedule name.	string	Maximum length: 31																			
start	Time of day to start the schedule, format hh:mm.	user	Not Specified																			
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000																		

config firewall security-policy

Configure NGFW IPv4/IPv6 application policies.

```

config firewall security-policy
    Description: Configure NGFW IPv4/IPv6 application policies.
    edit <policyid>
        set action [accept|deny]
        set app-category <id1>, <id2>, ...
        set app-group <name1>, <name2>, ...
        set application <id1>, <id2>, ...
        set application-list {string}
        set av-profile {string}
        set casb-profile {string}
        set comments {var-string}
        set diameter-filter-profile {string}
        set dlp-profile {string}
        set dnsfilter-profile {string}
        set dstaddr <name1>, <name2>, ...
        set dstaddr-negate [enable|disable]
        set dstaddr6 <name1>, <name2>, ...
        set dstaddr6-negate [enable|disable]
        set dstintf <name1>, <name2>, ...
        set emailfilter-profile {string}
        set enforce-default-app-port [enable|disable]
        set file-filter-profile {string}
        set fsso-groups <name1>, <name2>, ...
        set groups <name1>, <name2>, ...
        set icap-profile {string}
        set internet-service [enable|disable]
        set internet-service-custom <name1>, <name2>, ...
        set internet-service-custom-group <name1>, <name2>, ...
        set internet-service-group <name1>, <name2>, ...
        set internet-service-name <name1>, <name2>, ...
        set internet-service-negate [enable|disable]
        set internet-service-src [enable|disable]
        set internet-service-src-custom <name1>, <name2>, ...
        set internet-service-src-custom-group <name1>, <name2>, ...
        set internet-service-src-group <name1>, <name2>, ...
        set internet-service-src-name <name1>, <name2>, ...
        set internet-service-src-negate [enable|disable]
        set internet-service6 [enable|disable]
        set internet-service6-custom <name1>, <name2>, ...
        set internet-service6-custom-group <name1>, <name2>, ...
        set internet-service6-group <name1>, <name2>, ...
        set internet-service6-name <name1>, <name2>, ...
        set internet-service6-negate [enable|disable]
        set internet-service6-src [enable|disable]
        set internet-service6-src-custom <name1>, <name2>, ...
        set internet-service6-src-custom-group <name1>, <name2>, ...
        set internet-service6-src-group <name1>, <name2>, ...
        set internet-service6-src-name <name1>, <name2>, ...
        set internet-service6-src-negate [enable|disable]
        set ips-sensor {string}
        set ips-voip-filter {string}
        set learning-mode [enable|disable]

```

```

set logtraffic [all|utm|...]
set name {string}
set nat46 [enable|disable]
set nat64 [enable|disable]
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set schedule {string}
set sctp-filter-profile {string}
set send-deny-packet [disable|enable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcaddr6 <name1>, <name2>, ...
set srcaddr6-negate [enable|disable]
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssl-ssh-profile {string}
set status [enable|disable]
set telemetry-profile {string}
set url-category {user}
set users <name1>, <name2>, ...
set uuid {uuid}
set videofilter-profile {string}
set virtual-patch-profile {string}
set voip-profile {string}
set webfilter-profile {string}
next
end

```

config firewall security-policy

Parameter	Description	Type	Size	Default
action	Policy action (accept/deny).	option	-	deny
	Option	Description		
	<i>accept</i>	Allows session that match the firewall policy.		
	<i>deny</i>	Blocks sessions that match the firewall policy.		
app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	Application group names. Application group names.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
application- list	Name of an existing Application list.	string	Maximum length: 47							
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 47							
casb-profile	Name of an existing CASB profile.	string	Maximum length: 47							
comments	Comment.	var-string	Maximum length: 1023							
diameter- filter-profile	Name of an existing Diameter filter profile.	string	Maximum length: 47							
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 47							
dnsfilter- profile	Name of an existing DNS filter profile.	string	Maximum length: 47							
dstaddr <name>	Destination IPv4 address name and address group names. Address name.	string	Maximum length: 79							
dstaddr- negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable destination address negate.</td></tr><tr><td>disable</td><td>Disable destination address negate.</td></tr></table>				Option	Description	enable	Enable destination address negate.	disable	Disable destination address negate.
Option	Description									
enable	Enable destination address negate.									
disable	Disable destination address negate.									
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79							
dstaddr6- negate	When enabled dstaddr6 specifies what the destination address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPv6 destination address negate.</td></tr><tr><td>disable</td><td>Disable IPv6 destination address negate.</td></tr></table>				Option	Description	enable	Enable IPv6 destination address negate.	disable	Disable IPv6 destination address negate.
Option	Description									
enable	Enable IPv6 destination address negate.									
disable	Disable IPv6 destination address negate.									

Parameter	Description	Type	Size	Default						
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79							
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 47							
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 47							
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511							
groups <name>	Names of user groups that can authenticate with this policy. User group name.	string	Maximum length: 79							
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 47							
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address, service and default application port enforcement are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.
Option	Description									
<i>enable</i>	Enable use of Internet Services in policy.									
<i>disable</i>	Disable use of Internet Services in policy.									
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79							
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service match.</td></tr></table>				Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.
Option	Description									
<i>enable</i>	Enable negated Internet Service match.									
<i>disable</i>	Disable negated Internet Service match.									
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services source in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services source in policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of Internet Services source in policy.	<i>disable</i>	Disable use of Internet Services source in policy.
Option	Description									
<i>enable</i>	Enable use of Internet Services source in policy.									
<i>disable</i>	Disable use of Internet Services source in policy.									
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service source match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service source match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated Internet Service source match.	<i>disable</i>	Disable negated Internet Service source match.			
Option	Description									
<i>enable</i>	Enable negated Internet Service source match.									
<i>disable</i>	Disable negated Internet Service source match.									
internet-service6	Enable/disable use of IPv6 Internet Services for this policy. If enabled, destination address, service and default application port enforcement are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of IPv6 Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of IPv6 Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of IPv6 Internet Services in policy.	<i>disable</i>	Disable use of IPv6 Internet Services in policy.			
Option	Description									
<i>enable</i>	Enable use of IPv6 Internet Services in policy.									
<i>disable</i>	Disable use of IPv6 Internet Services in policy.									
internet-service6-custom <name>	Custom IPv6 Internet Service name. Custom IPv6 Internet Service name.	string	Maximum length: 79							
internet-service6-custom-group <name>	Custom IPv6 Internet Service group name. Custom IPv6 Internet Service group name.	string	Maximum length: 79							
internet-service6-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service6-name <name>	IPv6 Internet Service name. IPv6 Internet Service name.	string	Maximum length: 79							
internet-service6-negate	When enabled internet-service6 specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated IPv6 Internet Service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated IPv6 Internet Service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated IPv6 Internet Service match.	<i>disable</i>	Disable negated IPv6 Internet Service match.			
Option	Description									
<i>enable</i>	Enable negated IPv6 Internet Service match.									
<i>disable</i>	Disable negated IPv6 Internet Service match.									
internet-service6-src	Enable/disable use of IPv6 Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable use of IPv6 Internet Services source in policy.		
	<i>disable</i>	Disable use of IPv6 Internet Services source in policy.		
internet-service6-src-custom <name>	Custom IPv6 Internet Service source name. Custom Internet Service name.	string	Maximum length: 79	
internet-service6-src-custom-group <name>	Custom Internet Service6 source group name. Custom Internet Service6 group name.	string	Maximum length: 79	
internet-service6-src-group <name>	Internet Service6 source group name. Internet Service group name.	string	Maximum length: 79	
internet-service6-src-name <name>	IPv6 Internet Service source name. Internet Service name.	string	Maximum length: 79	
internet-service6-src-negate	When enabled internet-service6-src specifies what the service must NOT be.	option	-	disable
	Option Description			
	<i>enable</i>	Enable negated IPv6 Internet Service source match.		
	<i>disable</i>	Disable negated IPv6 Internet Service source match.		
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 47	
ips-voip-filter	Name of an existing VoIP (ips) profile.	string	Maximum length: 47	
learning-mode	Enable to allow everything, but log all of the meaningful data for security information gathering. A learning report will be generated.	option	-	disable
	Option Description			
	<i>enable</i>	Enable learning mode.		
	<i>disable</i>	Disable learning mode.		

Parameter	Description	Type	Size	Default								
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
name	Policy name.	string	Maximum length: 35									
nat46	Enable/disable NAT46.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NAT46.</td></tr><tr><td><i>disable</i></td><td>Disable NAT46.</td></tr></table>	Option	Description	<i>enable</i>	Enable NAT46.	<i>disable</i>	Disable NAT46.					
Option	Description											
<i>enable</i>	Enable NAT46.											
<i>disable</i>	Disable NAT46.											
nat64	Enable/disable NAT64.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NAT64.</td></tr><tr><td><i>disable</i></td><td>Disable NAT64.</td></tr></table>	Option	Description	<i>enable</i>	Enable NAT64.	<i>disable</i>	Disable NAT64.					
Option	Description											
<i>enable</i>	Enable NAT64.											
<i>disable</i>	Disable NAT64.											
policyid	Policy ID.	integer	Minimum value: 0 0 Maximum value: 4294967294									
profile-group	Name of profile group.	string	Maximum length: 47									
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 47	default								
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single</i></td><td>Do not allow security profile groups.</td></tr><tr><td><i>group</i></td><td>Allow security profile groups.</td></tr></table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.					
Option	Description											
<i>single</i>	Do not allow security profile groups.											
<i>group</i>	Allow security profile groups.											

Parameter	Description	Type	Size	Default						
schedule	Schedule name.	string	Maximum length: 35							
sctp-filter-profile	Name of an existing SCTP filter profile.	string	Maximum length: 47							
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable deny-packet sending.</td></tr><tr><td>enable</td><td>Enable deny-packet sending.</td></tr></table>	Option	Description	disable	Disable deny-packet sending.	enable	Enable deny-packet sending.			
Option	Description									
disable	Disable deny-packet sending.									
enable	Enable deny-packet sending.									
service <name>	Service and service group names. Service name.	string	Maximum length: 79							
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated service match.</td></tr><tr><td>disable</td><td>Disable negated service match.</td></tr></table>	Option	Description	enable	Enable negated service match.	disable	Disable negated service match.			
Option	Description									
enable	Enable negated service match.									
disable	Disable negated service match.									
srcaddr <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source address negate.</td></tr><tr><td>disable</td><td>Disable source address negate.</td></tr></table>	Option	Description	enable	Enable source address negate.	disable	Disable source address negate.			
Option	Description									
enable	Enable source address negate.									
disable	Disable source address negate.									
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79							
srcaddr6-negate	When enabled srcaddr6 specifies what the source address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPv6 source address negate.</td></tr><tr><td>disable</td><td>Disable IPv6 source address negate.</td></tr></table>	Option	Description	enable	Enable IPv6 source address negate.	disable	Disable IPv6 source address negate.			
Option	Description									
enable	Enable IPv6 source address negate.									
disable	Disable IPv6 source address negate.									

Parameter	Description	Type	Size	Default						
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79							
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 47							
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 47	no-inspection						
status	Enable or disable this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
telemetry-profile *	Name of an existing telemetry profile.	string	Maximum length: 47							
url-category	URL categories or groups.	user	Not Specified							
users <name>	Names of individual users that can authenticate with this policy. User name.	string	Maximum length: 79							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000- 0000-0000- 000000000000						
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 47							
virtual-patch-profile	Name of an existing virtual-patch profile.	string	Maximum length: 47							
voip-profile	Name of an existing VoIP (voipd) profile.	string	Maximum length: 47							
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 47							

* This parameter may not exist in some models.

config firewall service category

Configure service categories.

```
config firewall service category
    Description: Configure service categories.
    edit <name>
        set comment {var-string}
```

```

        set fabric-object [enable|disable]
        set uuid {uuid}
    next
end

```

config firewall service category

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.
	Option	Description								
	<i>enable</i>	Object is set as a security fabric-wide global object.								
<i>disable</i>	Object is local to this security fabric member.									
name	Service category name.	string	Maximum length: 63							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

config firewall service custom

Configure custom services.

```

config firewall service custom
    Description: Configure custom services.
    edit <name>
        set app-category <id1>, <id2>, ...
        set app-service-type [disable|app-id|...]
        set application <id1>, <id2>, ...
        set category {string}
        set check-reset-range [disable|strict|...]
        set color {integer}
        set comment {var-string}
        set fabric-object [enable|disable]
        set fqdn {string}
        set helper [auto|disable|...]
        set icmpcode {integer}
        set icmptype {integer}
        set iprange {user}
        set protocol [TCP/UDP/UDP-Lite/SCTP|ICMP|...]
        set protocol-number {integer}
        set proxy [enable|disable]
    end
end

```



```

set sctp-portrange {user}
set session-ttl {user}
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-portrange {user}
set tcp-rst-timer {integer}
set tcp-timewait-timer {integer}
set udp-idle-timer {integer}
set udp-portrange {user}
set udplite-portrange {user}
set uuid {uuid}
next
end

```

config firewall service custom

Parameter	Description	Type	Size	Default
app-category <id>	Application category ID. Application category id.	integer	Minimum value: 0 Maximum value: 4294967295	
app-service- type	Application service type.	option	-	disable
	Option	Description		
	disable	Disable application type.		
	app-id	Application ID.		
	app-category	Applicatin category.		
application <id>	Application ID. Application id.	integer	Minimum value: 0 Maximum value: 4294967295	
category	Service category.	string	Maximum length: 63	
check-reset- range	Configure the type of ICMP error message verification.	option	-	default
	Option	Description		
	disable	Disable RST range check.		
	strict	Check RST range strictly.		
	default	Using system default setting.		

Parameter	Description	Type	Size	Default																																				
color	Color of icon on the GUI.	integer	Minimum value: 0 0 Maximum value: 32																																					
comment	Comment.	var-string	Maximum length: 255																																					
fabric-object	Security Fabric global object setting.	option	-	disable																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.																														
	Option	Description																																						
	<i>enable</i>	Object is set as a security fabric-wide global object.																																						
<i>disable</i>	Object is local to this security fabric member.																																							
fqdn	Fully qualified domain name.	string	Maximum length: 255																																					
helper	Helper name.	option	-	auto																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically select helper based on protocol and port.</td></tr><tr><td><i>disable</i></td><td>Disable helper.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>tftp</i></td><td>TFTP.</td></tr><tr><td><i>ras</i></td><td>RAS.</td></tr><tr><td><i>h323</i></td><td>H323.</td></tr><tr><td><i>tns</i></td><td>TNS.</td></tr><tr><td><i>mms</i></td><td>MMS.</td></tr><tr><td><i>sip</i></td><td>SIP.</td></tr><tr><td><i>pptp</i></td><td>PPTP.</td></tr><tr><td><i>rtsp</i></td><td>RTSP.</td></tr><tr><td><i>dns-udp</i></td><td>DNS UDP.</td></tr><tr><td><i>dns-tcp</i></td><td>DNS TCP.</td></tr><tr><td><i>pmap</i></td><td>PMAP.</td></tr><tr><td><i>rsh</i></td><td>RSH.</td></tr><tr><td><i>dcerpc</i></td><td>DCERPC.</td></tr><tr><td><i>mgcp</i></td><td>MGCP.</td></tr></table>				Option	Description	<i>auto</i>	Automatically select helper based on protocol and port.	<i>disable</i>	Disable helper.	<i>ftp</i>	FTP.	<i>tftp</i>	TFTP.	<i>ras</i>	RAS.	<i>h323</i>	H323.	<i>tns</i>	TNS.	<i>mms</i>	MMS.	<i>sip</i>	SIP.	<i>pptp</i>	PPTP.	<i>rtsp</i>	RTSP.	<i>dns-udp</i>	DNS UDP.	<i>dns-tcp</i>	DNS TCP.	<i>pmap</i>	PMAP.	<i>rsh</i>	RSH.	<i>dcerpc</i>	DCERPC.	<i>mgcp</i>	MGCP.
	Option	Description																																						
	<i>auto</i>	Automatically select helper based on protocol and port.																																						
	<i>disable</i>	Disable helper.																																						
	<i>ftp</i>	FTP.																																						
	<i>tftp</i>	TFTP.																																						
	<i>ras</i>	RAS.																																						
	<i>h323</i>	H323.																																						
	<i>tns</i>	TNS.																																						
	<i>mms</i>	MMS.																																						
	<i>sip</i>	SIP.																																						
	<i>pptp</i>	PPTP.																																						
	<i>rtsp</i>	RTSP.																																						
	<i>dns-udp</i>	DNS UDP.																																						
	<i>dns-tcp</i>	DNS TCP.																																						
	<i>pmap</i>	PMAP.																																						
	<i>rsh</i>	RSH.																																						
	<i>dcerpc</i>	DCERPC.																																						
<i>mgcp</i>	MGCP.																																							

Parameter	Description	Type	Size	Default
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255	
icmptype	ICMP type.	integer	Minimum value: 0 Maximum value: 4294967295	
iprange	Start and end of the IP range associated with service.	user	Not Specified	
name	Custom service name.	string	Maximum length: 79	
protocol	Protocol type based on IANA numbers.	option	-	TCP/UDP/UDP-Lite/SCTP
	Option		Description	
	TCP/UDP/UDP-Lite/SCTP		TCP, UDP, UDP-Lite and SCTP.	
	ICMP		ICMP.	
	ICMP6		ICMP6.	
	IP		IP.	
	HTTP		HTTP - for web proxy.	
	FTP		FTP - for web proxy.	
	CONNECT		Connect - for web proxy.	
	SOCKS-TCP		Socks TCP - for web proxy.	
	SOCKS-UDP		Socks UDP - for web proxy.	
	ALL		All - for web proxy.	
protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254	
proxy	Enable/disable web proxy service.	option	-	disable
	Option		Description	
	enable		Enable setting.	
	disable		Disable setting.	
sctp-portrange	Multiple SCTP port ranges.	user	Not Specified	

Parameter	Description	Type	Size	Default
session-ttl	Session TTL (300 - 2764800, 0 = default).	user	Not Specified	
tcp-halfclose-timer	Wait time to close a TCP session waiting for an unanswered FIN packet (1 - 86400 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 86400	
tcp-halfopen-timer	Wait time to close a TCP session waiting for an unanswered open session packet (1 - 86400 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 86400	
tcp-portrange	Multiple TCP port ranges.	user	Not Specified	
tcp-rst-timer	Set the length of the TCP CLOSE state in seconds (5 - 300 sec, 0 = default).	integer	Minimum value: 5 Maximum value: 300	
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds (1 - 300 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 300	
udp-idle-timer	Number of seconds before an idle UDP/UDP-Lite connection times out (0 - 86400 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 86400	
udp-portrange	Multiple UDP port ranges.	user	Not Specified	
udplite-portrange	Multiple UDP-Lite port ranges.	user	Not Specified	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config firewall service group

Configure service groups.

```
config firewall service group
  Description: Configure service groups.
  edit <name>
    set color {integer}
    set comment {var-string}
    set fabric-object [enable|disable]
    set member <name1>, <name2>, ...
    set proxy [enable|disable]
    set uuid {uuid}
  next
end
```

config firewall service group

Parameter	Description	Type	Size	Default						
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
comment	Comment.	var-string	Maximum length: 255							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td>disable</td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	enable	Object is set as a security fabric-wide global object.	disable	Object is local to this security fabric member.
Option	Description									
enable	Object is set as a security fabric-wide global object.									
disable	Object is local to this security fabric member.									
member <name>	Service objects contained within the group. Service or service group name.	string	Maximum length: 79							
name	Service group name.	string	Maximum length: 79							
proxy	Enable/disable web proxy service group.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

config firewall shaper per-ip-shaper

Configure per-IP traffic shaper.

```
config firewall shaper per-ip-shaper
  Description: Configure per-IP traffic shaper.
  edit <name>
    set bandwidth-unit [kpbs|mbps|...]
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
    set max-bandwidth {integer}
    set max-concurrent-session {integer}
```

```

        set max-concurrent-tcp-session {integer}
        set max-concurrent-udp-session {integer}
    next
end

```

config firewall shaper per-ip-shaper

Parameter	Description	Type	Size	Default
bandwidth-unit	Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps
	Option	Description		
	<i>kbps</i>	Kilobits per second.		
	<i>mbps</i>	Megabits per second.		
	<i>gbps</i>	Gigabits per second.		
diffserv-forward	Enable/disable changing the Forward (original) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting forward (original) traffic DiffServ.		
	<i>disable</i>	Disable setting forward (original) traffic DiffServ.		
diffserv-reverse	Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.		
	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.		
diffservcode-forward	Forward (original) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified	
diffservcode-rev	Reverse (reply) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified	
max-bandwidth	Upper bandwidth limit enforced by this shaper (0 - 80000000). 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000 **	0

Parameter	Description	Type	Size	Default
max-concurrent-session	Maximum number of concurrent sessions allowed by this shaper (0 - 2097000). 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0
max-concurrent-tcp-session	Maximum number of concurrent TCP sessions allowed by this shaper (0 - 2097000). 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0
max-concurrent-udp-session	Maximum number of concurrent UDP sessions allowed by this shaper (0 - 2097000). 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0
name	Traffic shaper name.	string	Maximum length: 35	

** Values may differ between models.

config firewall shaper traffic-shaper

Configure shared traffic shaper.

```

config firewall shaper traffic-shaper
  Description: Configure shared traffic shaper.
  edit <name>
    set bandwidth-unit [kbps|mbps|...]
    set cos {user}
    set cos-marking [enable|disable]
    set cos-marking-method [multi-stage|static]
    set diffserv [enable|disable]
    set diffservcode {user}
    set dscp-marking-method [multi-stage|static]
    set exceed-bandwidth {integer}
    set exceed-class-id {integer}
    set exceed-cos {user}
    set exceed-dscp {user}
    set guaranteed-bandwidth {integer}
    set maximum-bandwidth {integer}
    set maximum-cos {user}
    set maximum-dscp {user}
    set overhead {integer}
    set per-policy [disable|enable]
    set priority [low|medium|...]

```

```
next
end
```

config firewall shaper traffic-shaper

Parameter	Description	Type	Size	Default								
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>kbps</td><td>Kilobits per second.</td></tr><tr><td>mbps</td><td>Megabits per second.</td></tr><tr><td>gbps</td><td>Gigabits per second.</td></tr></table>	Option	Description	kbps	Kilobits per second.	mbps	Megabits per second.	gbps	Gigabits per second.			
Option	Description											
kbps	Kilobits per second.											
mbps	Megabits per second.											
gbps	Gigabits per second.											
cos	VLAN CoS mark.	user	Not Specified									
cos-marking	Enable/disable VLAN CoS marking.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable VLAN CoS marking.</td></tr><tr><td>disable</td><td>Disable VLAN CoS marking.</td></tr></table>	Option	Description	enable	Enable VLAN CoS marking.	disable	Disable VLAN CoS marking.					
Option	Description											
enable	Enable VLAN CoS marking.											
disable	Disable VLAN CoS marking.											
cos-marking-method	Select VLAN CoS marking method.	option	-	static								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>multi-stage</td><td>Multi stage marking.</td></tr><tr><td>static</td><td>Static marking.</td></tr></table>	Option	Description	multi-stage	Multi stage marking.	static	Static marking.					
Option	Description											
multi-stage	Multi stage marking.											
static	Static marking.											
diffserv	Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting traffic DiffServ.</td></tr><tr><td>disable</td><td>Disable setting traffic DiffServ.</td></tr></table>	Option	Description	enable	Enable setting traffic DiffServ.	disable	Disable setting traffic DiffServ.					
Option	Description											
enable	Enable setting traffic DiffServ.											
disable	Disable setting traffic DiffServ.											
diffservcode	DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified									
dscp-marking-method	Select DSCP marking method.	option	-	static								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>multi-stage</i>	Multistage marking.		
	<i>static</i>	Static marking.		
exceed-bandwidth	Exceed bandwidth used for DSCP/VLAN CoS multi-stage marking. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 0 Maximum value: 80000000 **	
exceed-class-id	Class ID for traffic in guaranteed-bandwidth and maximum-bandwidth.	integer	Minimum value: 0 0 Maximum value: 4294967295	
exceed-cos	VLAN CoS mark for traffic in [guaranteed-bandwidth, exceed-bandwidth].	user	Not Specified	
exceed-dscp	DSCP mark for traffic in guaranteed-bandwidth and exceed-bandwidth.	user	Not Specified	
guaranteed-bandwidth	Amount of bandwidth guaranteed for this shaper (0 - 80000000). Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 0 Maximum value: 80000000 **	
maximum-bandwidth	Upper bandwidth limit enforced by this shaper (0 - 80000000). 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 0 Maximum value: 80000000 **	
maximum-cos	VLAN CoS mark for traffic in [exceed-bandwidth, maximum-bandwidth].	user	Not Specified	
maximum-dscp	DSCP mark for traffic in exceed-bandwidth and maximum-bandwidth.	user	Not Specified	
name	Traffic shaper name.	string	Maximum length: 35	
overhead	Per-packet size overhead used in rate computations.	integer	Minimum value: 0 0 Maximum value: 100	
per-policy	Enable/disable applying a separate shaper for each policy. For example, if enabled the guaranteed bandwidth is applied separately for each policy.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	All referring policies share one traffic shaper.		
	<i>enable</i>	Each referring policy has its own traffic shaper.		
priority	Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.	option	-	high
	Option	Description		
	<i>low</i>	Low priority.		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		

** Values may differ between models.

config firewall shaping-policy

Configure shaping policies.

```
config firewall shaping-policy
  Description: Configure shaping policies.
  edit <id>
    set app-category <id1>, <id2>, ...
    set app-group <name1>, <name2>, ...
    set application <id1>, <id2>, ...
    set class-id {integer}
    set comment {var-string}
    set cos {user}
    set cos-mask {user}
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
    set dstaddr <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set groups <name1>, <name2>, ...
    set internet-service [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-name <name1>, <name2>, ...
    set internet-service-src [enable|disable]
    set internet-service-src-custom <name1>, <name2>, ...
```

```

set internet-service-src-custom-group <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-name <name1>, <name2>, ...
set ip-version [4|6]
set name {string}
set per-ip-shaper {string}
set schedule {string}
set service <name1>, <name2>, ...
set srcaddr <name1>, <name2>, ...
set srcaddr6 <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set status [enable|disable]
set tos {user}
set tos-mask {user}
set tos-negate [enable|disable]
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set traffic-type [forwarding|local-in|...]
set url-category <id1>, <id2>, ...
set users <name1>, <name2>, ...
set uuid {uuid}
next
end

```

config firewall shaping-policy

Parameter	Description	Type	Size	Default
app-category <id>	IDs of one or more application categories that this shaper applies application control traffic shaping to. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	One or more application group names. Application group name.	string	Maximum length: 79	
application <id>	IDs of one or more applications that this shaper applies application control traffic shaping to. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	
comment	Comments.	var-string	Maximum length: 255	
cos	VLAN CoS bit pattern.	user	Not Specified	

Parameter	Description	Type	Size	Default						
cos-mask	VLAN CoS evaluated bits.	user	Not Specified							
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting forward (original) traffic DiffServ.</td></tr><tr><td>disable</td><td>Disable setting forward (original) traffic DiffServ.</td></tr></table>	Option	Description	enable	Enable setting forward (original) traffic DiffServ.	disable	Disable setting forward (original) traffic DiffServ.			
Option	Description									
enable	Enable setting forward (original) traffic DiffServ.									
disable	Disable setting forward (original) traffic DiffServ.									
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting reverse (reply) traffic DiffServ.</td></tr><tr><td>disable</td><td>Disable setting reverse (reply) traffic DiffServ.</td></tr></table>	Option	Description	enable	Enable setting reverse (reply) traffic DiffServ.	disable	Disable setting reverse (reply) traffic DiffServ.			
Option	Description									
enable	Enable setting reverse (reply) traffic DiffServ.									
disable	Disable setting reverse (reply) traffic DiffServ.									
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified							
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified							
dstaddr <name>	IPv4 destination address and address group names. Address name.	string	Maximum length: 79							
dstaddr6 <name>	IPv6 destination address and address group names. Address name.	string	Maximum length: 79							
dstintf <name>	One or more outgoing (egress) interfaces. Interface name.	string	Maximum length: 79							
groups <name>	Apply this traffic shaping policy to user groups that have authenticated with the FortiGate. Group name.	string	Maximum length: 79							
id	Shaping policy ID (0 - 4294967295).	integer	Minimum value: 0 0 Maximum value: 4294967295							

Parameter	Description	Type	Size	Default						
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Service in shaping-policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Service in shaping-policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Service in shaping-policy.	<i>disable</i>	Disable use of Internet Service in shaping-policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Service in shaping-policy.									
<i>disable</i>	Disable use of Internet Service in shaping-policy.									
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-name <name>	Internet Service ID. Internet Service name.	string	Maximum length: 79							
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Service source in shaping-policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Service source in shaping-policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Service source in shaping-policy.	<i>disable</i>	Disable use of Internet Service source in shaping-policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Service source in shaping-policy.									
<i>disable</i>	Disable use of Internet Service source in shaping-policy.									
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							
ip-version	Apply this traffic shaping policy to IPv4 or IPv6 traffic.	option	-	4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for Configuration Method.</td></tr><tr><td>6</td><td>Use IPv6 addressing for Configuration Method.</td></tr></table>	Option	Description	4	Use IPv4 addressing for Configuration Method.	6	Use IPv6 addressing for Configuration Method.			
Option	Description									
4	Use IPv4 addressing for Configuration Method.									
6	Use IPv6 addressing for Configuration Method.									
name	Shaping policy name.	string	Maximum length: 35							
per-ip-shaper	Per-IP traffic shaper to apply with this policy.	string	Maximum length: 35							
schedule	Schedule name.	string	Maximum length: 35							
service <name>	Service and service group names. Service name.	string	Maximum length: 79							
srcaddr <name>	IPv4 source address and address group names. Address name.	string	Maximum length: 79							
srcaddr6 <name>	IPv6 source address and address group names. Address name.	string	Maximum length: 79							
srcintf <name>	One or more incoming (ingress) interfaces. Interface name.	string	Maximum length: 79							
status	Enable/disable this traffic shaping policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable traffic shaping policy.</td></tr><tr><td>disable</td><td>Disable traffic shaping policy.</td></tr></table>	Option	Description	enable	Enable traffic shaping policy.	disable	Disable traffic shaping policy.			
Option	Description									
enable	Enable traffic shaping policy.									
disable	Disable traffic shaping policy.									
tos	ToS (Type of Service) value used for comparison.	user	Not Specified							
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified							

Parameter	Description	Type	Size	Default								
tos-negate	Enable negated TOS match.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable TOS match negate.</td></tr><tr><td>disable</td><td>Disable TOS match negate.</td></tr></table>				Option	Description	enable	Enable TOS match negate.	disable	Disable TOS match negate.		
	Option	Description										
	enable	Enable TOS match negate.										
disable	Disable TOS match negate.											
traffic-shaper	Traffic shaper to apply to traffic forwarded by the firewall policy.	string	Maximum length: 35									
traffic-shaper-reverse	Traffic shaper to apply to response traffic received by the firewall policy.	string	Maximum length: 35									
traffic-type	Traffic type.	option	-	forwarding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>forwarding</td><td>Forwarding traffic.</td></tr><tr><td>local-in</td><td>Local-in traffic.</td></tr><tr><td>local-out</td><td>Local-out traffic.</td></tr></table>				Option	Description	forwarding	Forwarding traffic.	local-in	Local-in traffic.	local-out	Local-out traffic.
	Option	Description										
	forwarding	Forwarding traffic.										
	local-in	Local-in traffic.										
local-out	Local-out traffic.											
url-category <id>	IDs of one or more FortiGuard Web Filtering categories that this shaper applies traffic shaping to. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295									
users <name>	Apply this traffic shaping policy to individual users that have authenticated with the FortiGate. User name.	string	Maximum length: 79									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000								

config firewall shaping-profile

Configure shaping profiles.

```
config firewall shaping-profile
  Description: Configure shaping profiles.
  edit <profile-name>
    set comment {var-string}
    set default-class-id {integer}
    set npu-offloading [disable|enable]
    config shaping-entries
      Description: Define shaping entries of this shaping profile.
      edit <id>
```

```

        set burst-in-msec {integer}
        set cburst-in-msec {integer}
        set class-id {integer}
        set guaranteed-bandwidth-percentage {integer}
        set limit {integer}
        set max {integer}
        set maximum-bandwidth-percentage {integer}
        set min {integer}
        set priority [top|critical|...]
        set red-probability {integer}
    next
end
    set type [policing|queuing]
next
end

```

config firewall shaping-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
default-class-id	Default class ID to handle unclassified packets (including all local traffic).	integer	Minimum value: 0 Maximum value: 4294967295	0
npu-offloading	Enable/disable NPU offloading.	option	-	enable
	Option		Description	
	<i>disable</i>		Diable shaper offloading.	
	<i>enable</i>		Enable shaper offloading.	
profile-name	Shaping profile name.	string	Maximum length: 35	
type	Select shaping profile type: policing / queuing.	option	-	policing
	Option		Description	
	<i>policing</i>		Enable policing mode.	
	<i>queuing</i>		Enable queuing mode.	

config shaping-entries

Parameter	Description	Type	Size	Default
burst-in-msec	Number of bytes that can be burst at maximum-bandwidth speed. Formula: burst = maximum-bandwidth*burst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
cburst-in-msec	Number of bytes that can be burst as fast as the interface can transmit. Formula: cburst = maximum-bandwidth*cburst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
class-id	Class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
guaranteed-bandwidth-percentage	Guaranteed bandwidth in percentage.	integer	Minimum value: 0 Maximum value: 100	0
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295	0
limit	Hard limit on the real queue size in packets.	integer	Minimum value: 5 Maximum value: 10000	100
max	Average queue size in packets at which RED drop probability is maximal.	integer	Minimum value: 3 Maximum value: 3000	250
maximum-bandwidth-percentage	Maximum bandwidth in percentage.	integer	Minimum value: 1 Maximum value: 100	1
min	Average queue size in packets at which RED drop becomes a possibility.	integer	Minimum value: 3 Maximum value: 3000	83
priority	Priority.	option	-	high
	Option	Description		
	top	Top priority.		
	critical	Critical priority.		
	high	High priority.		
	medium	Medium priority.		
	low	Low priority.		

Parameter	Description	Type	Size	Default
red-probability	Maximum probability (in percentage) for RED marking.	integer	Minimum value: 0 Maximum value: 20	0

config firewall sniffer

Configure sniffer.

```

config firewall sniffer
  Description: Configure sniffer.
  edit <id>
    config anomaly
      Description: Configuration method to edit Denial of Service (DoS) anomaly settings.
      edit <name>
        set action [pass|block]
        set log [enable|disable]
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set status [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
      next
    end
    set application-list {string}
    set application-list-status [enable|disable]
    set av-profile {string}
    set av-profile-status [enable|disable]
    set dlp-profile {string}
    set dlp-profile-status [enable|disable]
    set dsri [enable|disable]
    set emailfilter-profile {string}
    set emailfilter-profile-status [enable|disable]
    set file-filter-profile {string}
    set file-filter-profile-status [enable|disable]
    set host {string}
    set interface {string}
    set ip-threatfeed <name1>, <name2>, ...
    set ip-threatfeed-status [enable|disable]
    set ips-dos-status [enable|disable]
    set ips-sensor {string}
    set ips-sensor-status [enable|disable]
    set ipv6 [enable|disable]
    set logtraffic [all|utm|...]
    set non-ip [enable|disable]
    set port {string}
    set protocol {string}
    set status [enable|disable]
  
```

```

set uuid {uuid}
set vlan {string}
set webfilter-profile {string}
set webfilter-profile-status [enable|disable]
next
end

```

config firewall sniffer

Parameter	Description	Type	Size	Default						
application-list	Name of an existing application list.	string	Maximum length: 47							
application-list-status	Enable/disable application control profile.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
av-profile	Name of an existing antivirus profile.	string	Maximum length: 47							
av-profile-status	Enable/disable antivirus profile.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 47							
dlp-profile-status	Enable/disable DLP profile.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dsri	Enable/disable DSRI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DSRI.</td></tr><tr><td><i>disable</i></td><td>Disable DSRI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.			
Option	Description									
<i>enable</i>	Enable DSRI.									
<i>disable</i>	Disable DSRI.									

Parameter	Description	Type	Size	Default						
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 47							
emailfilter-profile-status	Enable/disable emailfilter.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 47							
file-filter-profile-status	Enable/disable file filter.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
host	Hosts to filter for in sniffer traffic (Format examples: 1.1.1.1, 2.2.2.0/24, 3.3.3.3/255.255.255.0, 4.4.4.0-4.4.4.240).	string	Maximum length: 63							
id	Sniffer ID (0 - 9999).	integer	Minimum value: 0 Maximum value: 9999	0						
interface	Interface name that traffic sniffing will take place on.	string	Maximum length: 35							
ip-threatfeed <name>	Name of an existing IP threat feed. Threat feed name.	string	Maximum length: 79							
ip-threatfeed-status	Enable/disable IP threat feed.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
ips-dos-status	Enable/disable IPS DoS anomaly detection.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 47	
ips-sensor-status	Enable/disable IPS sensor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ipv6	Enable/disable sniffing IPv6 packets.	option	-	disable
	Option Description			
	<i>enable</i>	Enable sniffer for IPv6 packets.		
	<i>disable</i>	Disable sniffer for IPv6 packets.		
logtraffic	Either log all sessions, only sessions that have a security profile applied, or disable all logging for this policy.	option	-	utm
	Option Description			
	<i>all</i>	Log all sessions accepted or denied by this policy.		
	<i>utm</i>	Log traffic that has a security profile applied to it.		
	<i>disable</i>	Disable all logging for this policy.		
non-ip	Enable/disable sniffing non-IP packets.	option	-	disable
	Option Description			
	<i>enable</i>	Enable sniffer for non-IP packets.		
	<i>disable</i>	Disable sniffer for non-IP packets.		
port	Ports to sniff (Format examples: 10, :20, 30:40, 50-, 100-200).	string	Maximum length: 63	
protocol	Integer value for the protocol type as defined by IANA (0 - 255).	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of the sniffer.	option	-	enable
	Option Description			
	<i>enable</i>	Enable sniffer status.		
	<i>disable</i>	Disable sniffer status.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
vlan	List of VLANs to sniff.	string	Maximum length: 63	
webfilter-profile	Name of an existing web filter profile.	string	Maximum length: 47	
webfilter-profile-status	Enable/disable web filter profile.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config anomaly

Parameter	Description	Type	Size	Default
action	Action taken when the threshold is reached.	option	-	pass
	Option Description			
	<i>pass</i>	Allow traffic but record a log message if logging is enabled.		
	<i>block</i>	Block traffic if this anomaly is found.		
log	Enable/disable anomaly logging.	option	-	disable
	Option Description			
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
name	Anomaly name.	string	Maximum length: 63	
quarantine	Quarantine method.	option	-	none

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Quarantine is disabled.</td></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
	Option	Description								
	<i>none</i>	Quarantine is disabled.								
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. (Format ####d##h##m, minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine logging.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
	Option	Description								
	<i>disable</i>	Disable quarantine logging.								
<i>enable</i>	Enable quarantine logging.									
status	Enable/disable this anomaly.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this status.</td></tr><tr><td><i>enable</i></td><td>Enable this status.</td></tr></table>	Option	Description	<i>disable</i>	Disable this status.	<i>enable</i>	Enable this status.			
	Option	Description								
	<i>disable</i>	Disable this status.								
<i>enable</i>	Enable this status.									
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 0 1 Maximum value: 2147483647							
threshold (default)	Number of detected instances (packets per second or concurrent session number) which triggers action (1 - 2147483647, default = 1000). Note that each anomaly has a different threshold value assigned to it. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							

config firewall ssh host-key

SSH proxy host public keys.

```
config firewall ssh host-key
    Description: SSH proxy host public keys.
    edit <name>
        set hostname {string}
        set ip {ipv4-address-any}
        set nid [256|384|...]
```

```

set port {integer}
set public-key {var-string}
set status [trusted|revoked]
set type [RSA|DSA|...]
set usage [transparent-proxy|access-proxy]
next
end

```

config firewall ssh host-key

Parameter	Description	Type	Size	Default								
hostname	Hostname of the SSH server to match SSH certificate principals.	string	Maximum length: 255									
ip	IP address of the SSH server.	ipv4-address-any	Not Specified	0.0.0.0								
name	SSH public key name.	string	Maximum length: 35									
nid	Set the nid of the ECDSA key.	option	-	256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>256</td><td>The NID is ecdsa-sha2-nistp256.</td></tr><tr><td>384</td><td>The NID is ecdsa-sha2-nistp384.</td></tr><tr><td>521</td><td>The NID is ecdsa-sha2-nistp521.</td></tr></table>				Option	Description	256	The NID is ecdsa-sha2-nistp256.	384	The NID is ecdsa-sha2-nistp384.	521	The NID is ecdsa-sha2-nistp521.
Option	Description											
256	The NID is ecdsa-sha2-nistp256.											
384	The NID is ecdsa-sha2-nistp384.											
521	The NID is ecdsa-sha2-nistp521.											
port	Port of the SSH server.	integer	Minimum value: 22 0 Maximum value: 4294967295									
public-key	SSH public key.	var-string	Maximum length: 32768									
status	Set the trust status of the public key.	option	-	trusted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>trusted</td><td>The public key is trusted.</td></tr><tr><td>revoked</td><td>The public key is revoked.</td></tr></table>				Option	Description	trusted	The public key is trusted.	revoked	The public key is revoked.		
Option	Description											
trusted	The public key is trusted.											
revoked	The public key is revoked.											
type	Set the type of the public key.	option	-	RSA								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>RSA</td><td>The type of the public key is RSA.</td></tr></table>				Option	Description	RSA	The type of the public key is RSA.				
Option	Description											
RSA	The type of the public key is RSA.											

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>DSA</td><td>The type of the public key is DSA.</td></tr><tr><td>ECDSA</td><td>The type of the public key is ECDSA.</td></tr><tr><td>ED25519</td><td>The type of the public key is ED25519.</td></tr><tr><td>RSA-CA</td><td>The type of the public key is from RSA CA.</td></tr><tr><td>DSA-CA</td><td>The type of the public key is from DSA CA.</td></tr><tr><td>ECDSA-CA</td><td>The type of the public key is from ECDSA CA.</td></tr><tr><td>ED25519-CA</td><td>The type of the public key is from ED25519 CA.</td></tr></table>	Option	Description	DSA	The type of the public key is DSA.	ECDSA	The type of the public key is ECDSA.	ED25519	The type of the public key is ED25519.	RSA-CA	The type of the public key is from RSA CA.	DSA-CA	The type of the public key is from DSA CA.	ECDSA-CA	The type of the public key is from ECDSA CA.	ED25519-CA	The type of the public key is from ED25519 CA.			
	Option	Description																		
	DSA	The type of the public key is DSA.																		
	ECDSA	The type of the public key is ECDSA.																		
	ED25519	The type of the public key is ED25519.																		
	RSA-CA	The type of the public key is from RSA CA.																		
	DSA-CA	The type of the public key is from DSA CA.																		
	ECDSA-CA	The type of the public key is from ECDSA CA.																		
ED25519-CA	The type of the public key is from ED25519 CA.																			
usage	Usage for this public key.	option	-	transparent-proxy																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>transparent-proxy</td><td>Transparent proxy uses this public key to validate server.</td></tr><tr><td>access-proxy</td><td>Access proxy uses this public key to validate server.</td></tr></table>	Option	Description	transparent-proxy	Transparent proxy uses this public key to validate server.	access-proxy	Access proxy uses this public key to validate server.													
	Option	Description																		
	transparent-proxy	Transparent proxy uses this public key to validate server.																		
access-proxy	Access proxy uses this public key to validate server.																			

config firewall ssh local-ca

SSH proxy local CA.

```
config firewall ssh local-ca
  Description: SSH proxy local CA.
  edit <name>
    set password {password}
    set private-key {user}
    set public-key {user}
    set source [built-in|user]
  next
end
```

config firewall ssh local-ca

Parameter	Description	Type	Size	Default
name	SSH proxy local CA name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local CA source type.	option	-	user
	Option	Description		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

config firewall ssh local-key

SSH proxy local keys.

```
config firewall ssh local-key
  Description: SSH proxy local keys.
  edit <name>
    set password {password}
    set private-key {user}
    set public-key {user}
    set source [built-in|user]
  next
end
```

config firewall ssh local-key

Parameter	Description	Type	Size	Default
name	SSH proxy local key name.	string	Maximum length: 35	
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local key source type.	option	-	user

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

config firewall ssh setting

SSH proxy settings.

```
config firewall ssh setting
    Description: SSH proxy settings.
    set caname {string}
    set host-trusted-checking [enable|disable]
    set hostkey-dsa1024 {string}
    set hostkey-ecdsa256 {string}
    set hostkey-ecdsa384 {string}
    set hostkey-ecdsa521 {string}
    set hostkey-ed25519 {string}
    set hostkey-rsa2048 {string}
    set untrusted-caname {string}
end
```

config firewall ssh setting

Parameter	Description	Type	Size	Default
caname	CA certificate used by SSH Inspection.	string	Maximum length: 35	
host-trusted-checking	Enable/disable host trusted checking.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable host key trusted checking.		
	<i>disable</i>	Disable host key trusted checking.		
hostkey-dsa1024	DSA certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa256	ECDSA nid256 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa384	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
hostkey-ecdsa521	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ed25519	ED25519 hostkey used by SSH proxy.	string	Maximum length: 35	
hostkey-rsa2048	RSA certificate used by SSH proxy.	string	Maximum length: 35	
untrusted-caname	Untrusted CA certificate used by SSH Inspection.	string	Maximum length: 35	

config firewall ssl setting

SSL proxy settings.

```
config firewall ssl setting
    Description: SSL proxy settings.
    set abbreviate-handshake [enable|disable]
    set cert-cache-capacity {integer}
    set cert-cache-timeout {integer}
    set cert-manager-cache-timeout {integer}
    set kxp-queue-threshold {integer}
    set no-matching-cipher-action [bypass|drop]
    set proxy-connect-timeout {integer}
    set resigned-short-lived-certificate [enable|disable]
    set session-cache-capacity {integer}
    set session-cache-timeout {integer}
    set ssl-dh-bits [768|1024|...]
    set ssl-queue-threshold {integer}
    set ssl-send-empty-frags [enable|disable]
end
```

config firewall ssl setting

Parameter	Description	Type	Size	Default
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of SSL abbreviated handshake.		
	<i>disable</i>	Disable use of SSL abbreviated handshake.		

Parameter	Description	Type	Size	Default						
cert-cache-capacity	Maximum capacity of the host certificate cache (0 - 500, default = 200).	integer	Minimum value: 0 Maximum value: 500	200						
cert-cache-timeout	Time limit to keep certificate cache (1 - 120 min, default = 10).	integer	Minimum value: 1 Maximum value: 120	10						
cert-manager-cache-timeout	Time limit for certificate manager to keep FortiGate re-signed server certificate (24 - 720 hours, default = 72).	integer	Minimum value: 24 Maximum value: 720	72						
kxp-queue-threshold *	Maximum length of the CP KXP queue. When the queue becomes full, the proxy switches cipher functions to the main CPU (0 - 512, default = 16).	integer	Minimum value: 0 Maximum value: 512	16						
no-matching-cipher-action	Bypass or drop the connection when no matching cipher is found.	option	-	bypass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass connection.</td></tr><tr><td>drop</td><td>Drop connection.</td></tr></table>				Option	Description	bypass	Bypass connection.	drop	Drop connection.
Option	Description									
bypass	Bypass connection.									
drop	Drop connection.									
proxy-connect-timeout	Time limit to make an internal connection to the appropriate proxy process (1 - 60 sec, default = 30).	integer	Minimum value: 1 Maximum value: 60	30						
resigned-short-lived-certificate	Enable/disable short-lived certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable short-lived certificate: re-signed certificate will remain valid until either the origin server certificate expires or cache timeouts.</td></tr><tr><td>disable</td><td>Disable short-lived certificate: re-signed certificate will have the same validation period as the origin server certificate.</td></tr></table>				Option	Description	enable	Enable short-lived certificate: re-signed certificate will remain valid until either the origin server certificate expires or cache timeouts.	disable	Disable short-lived certificate: re-signed certificate will have the same validation period as the origin server certificate.
Option	Description									
enable	Enable short-lived certificate: re-signed certificate will remain valid until either the origin server certificate expires or cache timeouts.									
disable	Disable short-lived certificate: re-signed certificate will have the same validation period as the origin server certificate.									
session-cache-capacity	Capacity of the SSL session cache (--Obsolete--) (1 - 1000, default = 500).	integer	Minimum value: 0 Maximum value: 1000	500						

Parameter	Description	Type	Size	Default
session-cache-timeout	Time limit to keep SSL session state (1 - 60 min, default = 20).	integer	Minimum value: 1 Maximum value: 60	20
ssl-dh-bits	Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).	option	-	2048
	Option Description			
	768	768-bit Diffie-Hellman prime.		
	1024	1024-bit Diffie-Hellman prime.		
	1536	1536-bit Diffie-Hellman prime.		
	2048	2048-bit Diffie-Hellman prime.		
ssl-queue-threshold *	Maximum length of the CP SSL queue. When the queue becomes full, the proxy switches cipher functions to the main CPU (0 - 512, default = 32).	integer	Minimum value: 0 Maximum value: 512	32
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV (for SSL 3.0 and TLS 1.0 only).	option	-	enable
	Option Description			
	enable	Send empty fragments.		
	disable	Do not send empty fragments.		

* This parameter may not exist in some models.

config firewall ssl-server

Configure SSL servers.

```
config firewall ssl-server
  Description: Configure SSL servers.
  edit <name>
    set add-header-x-forwarded-proto [enable|disable]
    set ip {ipv4-address-any}
    set mapped-port {integer}
    set port {integer}
    set ssl-algorithm [high|medium|...]
    set ssl-cert <name1>, <name2>, ...
    set ssl-client-renegotiation [allow|deny|...]
    set ssl-dh-bits [768|1024|...]
    set ssl-max-version [tls-1.0|tls-1.1|...]
    set ssl-min-version [tls-1.0|tls-1.1|...]
```

```

    set ssl-mode [half|full]
    set ssl-send-empty-frags [enable|disable]
    set url-rewrite [enable|disable]
next
end

```

config firewall ssl-server

Parameter	Description	Type	Size	Default
add-header-x-forwarded-proto	Enable/disable adding an X-Forwarded-Proto header to forwarded requests.	option	-	enable
	Option	Description		
	<i>enable</i>	Add X-Forwarded-Proto header.		
	<i>disable</i>	Do not add X-Forwarded-Proto header.		
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0
mapped-port	Mapped server service port (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535	80
name	Server name.	string	Maximum length: 35	
port	Server service port (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535	443
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	Option	Description		
	<i>high</i>	High encryption. Allow only AES and ChaCha		
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
ssl-cert <name>	List of certificate names to use for SSL connections to this server. (default = "Fortinet_SSL").	string	Maximum length: 79	

Parameter	Description	Type	Size	Default										
	Certificate list.													
ssl-client-renegotiation	Allow or block client renegotiation by server.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow a SSL client to renegotiate.</td></tr><tr><td><i>deny</i></td><td>Abort any SSL connection that attempts to renegotiate.</td></tr><tr><td><i>secure</i></td><td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td></tr></table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.					
Option	Description													
<i>allow</i>	Allow a SSL client to renegotiate.													
<i>deny</i>	Abort any SSL connection that attempts to renegotiate.													
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.													
ssl-dh-bits	Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).	option	-	2048										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.			
Option	Description													
<i>768</i>	768-bit Diffie-Hellman prime.													
<i>1024</i>	1024-bit Diffie-Hellman prime.													
<i>1536</i>	1536-bit Diffie-Hellman prime.													
<i>2048</i>	2048-bit Diffie-Hellman prime.													
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-	tls-1.3										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description													
<i>tls-1.0</i>	TLS 1.0.													
<i>tls-1.1</i>	TLS 1.1.													
<i>tls-1.2</i>	TLS 1.2.													
<i>tls-1.3</i>	TLS 1.3.													
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description													
<i>tls-1.0</i>	TLS 1.0.													
<i>tls-1.1</i>	TLS 1.1.													
<i>tls-1.2</i>	TLS 1.2.													
<i>tls-1.3</i>	TLS 1.3.													
ssl-mode	SSL/TLS mode for encryption and decryption of traffic.	option	-	full										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>half</i>	Client to FortiGate SSL.		
	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.		
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV.	option	-	enable
	Option	Description		
	<i>enable</i>	Send empty fragments.		
	<i>disable</i>	Do not send empty fragments.		
url-rewrite	Enable/disable rewriting the URL.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config firewall ssl-ssh-profile

Configure SSL/SSH protocol options.

```
config firewall ssl-ssh-profile
  Description: Configure SSL/SSH protocol options.
  edit <name>
    set allowlist [enable|disable]
    set block-blocklisted-certificates [disable|enable]
    set caname {string}
    set comment {var-string}
    config dot
      Description: Configure DNS over TLS options.
      set cert-validation-failure [allow|block|...]
      set cert-validation-timeout [allow|block|...]
      set client-certificate [bypass|inspect|...]
      set expired-server-cert [allow|block|...]
      set proxy-after-tcp-handshake [enable|disable]
      set quic [inspect|bypass|...]
      set revoked-server-cert [allow|block|...]
      set sni-server-cert-check [enable|strict|...]
      set status [disable|deep-inspection]
      set udp-not-quic [allow|block]
      set unsupported-ssl-cipher [allow|block]
      set unsupported-ssl-negotiation [allow|block]
      set unsupported-ssl-version [allow|block]
      set untrusted-server-cert [allow|block|...]
```

```

end
config ech-outer-sni
    Description: ClientHelloOuter SNIs to be blocked.
    edit <name>
        set sni {string}
    next
end
config ftps
    Description: Configure FTPS options.
    set cert-validation-failure [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set client-certificate [bypass|inspect|...]
    set expired-server-cert [allow|block|...]
    set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
    set ports {integer}
    set revoked-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set status [disable|deep-inspection]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set unsupported-ssl-version [allow|block]
    set untrusted-server-cert [allow|block|...]
end
config https
    Description: Configure HTTPS options.
    set cert-probe-failure [allow|block]
    set cert-validation-failure [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set client-certificate [bypass|inspect|...]
    set encrypted-client-hello [allow|block]
    set expired-server-cert [allow|block|...]
    set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set quic [inspect|bypass|...]
    set revoked-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set status [disable|certificate-inspection|...]
    set udp-not-quic [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set unsupported-ssl-version [allow|block]
    set untrusted-server-cert [allow|block|...]
end
config imaps
    Description: Configure IMAPS options.
    set cert-validation-failure [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set client-certificate [bypass|inspect|...]
    set expired-server-cert [allow|block|...]
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]

```

```

    set revoked-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set status [disable|deep-inspection]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set unsupported-ssl-version [allow|block]
    set untrusted-server-cert [allow|block|...]
end
set mapi-over-https [enable|disable]
config pop3s
    Description: Configure POP3S options.
    set cert-validation-failure [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set client-certificate [bypass|inspect|...]
    set expired-server-cert [allow|block|...]
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set revoked-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set status [disable|deep-inspection]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set unsupported-ssl-version [allow|block]
    set untrusted-server-cert [allow|block|...]
end
set rpc-over-https [enable|disable]
set server-cert <name1>, <name2>, ...
set server-cert-mode [re-sign|replace]
config smtps
    Description: Configure SMTPS options.
    set cert-validation-failure [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set client-certificate [bypass|inspect|...]
    set expired-server-cert [allow|block|...]
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set revoked-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set status [disable|deep-inspection]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set unsupported-ssl-version [allow|block]
    set untrusted-server-cert [allow|block|...]
end
config ssh
    Description: Configure SSH options.
    set inspect-all [disable|deep-inspection]
    set ports {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set ssh-algorithm [compatible|high-encryption]
    set ssh-tun-policy-check [disable|enable]
    set status [disable|deep-inspection]

```

```

        set unsupported-version [bypass|block]
    end
    config ssl
        Description: Configure SSL options.
        set cert-probe-failure [allow|block]
        set cert-validation-failure [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set client-certificate [bypass|inspect|...]
        set encrypted-client-hello [allow|block]
        set expired-server-cert [allow|block|...]
        set inspect-all [disable|certificate-inspection|...]
        set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
        set revoked-server-cert [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set unsupported-ssl-version [allow|block]
        set untrusted-server-cert [allow|block|...]
    end
    set ssl-anomaly-log [disable|enable]
    config ssl-exempt
        Description: Servers to exempt from SSL inspection.
        edit <id>
            set address {string}
            set address6 {string}
            set fortiguard-category {integer}
            set regex {string}
            set type [fortiguard-category|address|...]
            set wildcard-fqdn {string}
        next
    end
    set ssl-exemption-ip-rating [enable|disable]
    set ssl-exemption-log [disable|enable]
    set ssl-handshake-log [disable|enable]
    set ssl-negotiation-log [disable|enable]
    config ssl-server
        Description: SSL server settings used for client certificate request.
        edit <id>
            set ftps-client-certificate [bypass|inspect|...]
            set https-client-certificate [bypass|inspect|...]
            set imaps-client-certificate [bypass|inspect|...]
            set ip {ipv4-address-any}
            set pop3s-client-certificate [bypass|inspect|...]
            set smtps-client-certificate [bypass|inspect|...]
            set ssl-other-client-certificate [bypass|inspect|...]
        next
    end
    set ssl-server-cert-log [disable|enable]
    set supported-alpn [http1-1|http2|...]
    set untrusted-caname {string}
    set use-ssl-server [disable|enable]
next

```

end

config firewall ssl-ssh-profile

Parameter	Description	Type	Size	Default
allowlist	Enable/disable exempting servers by FortiGuard allowlist.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
block-blocklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blocklist.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable FortiGuard certificate blocklist.		
	<i>enable</i>	Enable FortiGuard certificate blocklist.		
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_SSL
comment	Optional comments.	var-string	Maximum length: 255	
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable inspection of MAPI over HTTPS.		
	<i>disable</i>	Disable inspection of MAPI over HTTPS.		
name	Name.	string	Maximum length: 47	
rpc-over-https	Enable/disable inspection of RPC over HTTPS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable inspection of RPC over HTTPS.		
	<i>disable</i>	Disable inspection of RPC over HTTPS.		
server-cert <name>	Certificate used by SSL Inspection to replace server certificate.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
	Certificate list.									
server-cert-mode	Re-sign or replace the server's certificate.	option	-	re-sign						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>re-sign</td><td>Multiple clients connecting to multiple servers.</td></tr><tr><td>replace</td><td>Protect an SSL server.</td></tr></table>	Option	Description	re-sign	Multiple clients connecting to multiple servers.	replace	Protect an SSL server.			
Option	Description									
re-sign	Multiple clients connecting to multiple servers.									
replace	Protect an SSL server.									
ssl-anomaly-log	Enable/disable logging of SSL anomalies.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of SSL anomalies.</td></tr><tr><td>enable</td><td>Enable logging of SSL anomalies.</td></tr></table>	Option	Description	disable	Disable logging of SSL anomalies.	enable	Enable logging of SSL anomalies.			
Option	Description									
disable	Disable logging of SSL anomalies.									
enable	Enable logging of SSL anomalies.									
ssl-exemption-ip-rating	Enable/disable IP based URL rating.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IP based URL rating.</td></tr><tr><td>disable</td><td>Disable IP based URL rating.</td></tr></table>	Option	Description	enable	Enable IP based URL rating.	disable	Disable IP based URL rating.			
Option	Description									
enable	Enable IP based URL rating.									
disable	Disable IP based URL rating.									
ssl-exemption-log	Enable/disable logging of SSL exemptions.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of SSL exemptions.</td></tr><tr><td>enable</td><td>Enable logging of SSL exemptions.</td></tr></table>	Option	Description	disable	Disable logging of SSL exemptions.	enable	Enable logging of SSL exemptions.			
Option	Description									
disable	Disable logging of SSL exemptions.									
enable	Enable logging of SSL exemptions.									
ssl-handshake-log	Enable/disable logging of TLS handshakes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of TLS handshakes.</td></tr><tr><td>enable</td><td>Enable logging of TLS handshakes.</td></tr></table>	Option	Description	disable	Disable logging of TLS handshakes.	enable	Enable logging of TLS handshakes.			
Option	Description									
disable	Disable logging of TLS handshakes.									
enable	Enable logging of TLS handshakes.									
ssl-negotiation-log	Enable/disable logging of SSL negotiation events.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging of SSL negotiation events.		
	<i>enable</i>	Enable logging of SSL negotiation events.		
ssl-server-cert-log	Enable/disable logging of server certificate information.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of server certificate information.		
	<i>enable</i>	Enable logging of server certificate information.		
supported-alpn	Configure ALPN option.	option	-	all
	Option	Description		
	<i>http1-1</i>	Enable all ALPN including HTTP1.1 except HTTP2 and SPDY.		
	<i>http2</i>	Enable all ALPN including HTTP2 except HTTP1.1 and SPDY.		
	<i>all</i>	Allow all ALPN extensions except SPDY.		
	<i>none</i>	Do not use ALPN.		
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_Untrusted
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-	disable
	Option	Description		
	<i>disable</i>	Don't use SSL server configuration.		
	<i>enable</i>	Use SSL server configuration.		

config dot

Parameter	Description	Type	Size	Default				
cert-validation-failure	Action based on certificate validation failure.	option	-	block				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr></table>				Option	Description	<i>allow</i>	Allow the server certificate.
Option	Description							
<i>allow</i>	Allow the server certificate.							

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
client-certificate	Action based on received client certificate.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
quic	QUIC inspection status (default = inspect).	option	-	inspect
	Option	Description		
	<i>inspect</i>	Inspect QUIC traffic.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass QUIC traffic.</td></tr><tr><td>block</td><td>Block QUIC traffic.</td></tr></table>	Option	Description	bypass	Bypass QUIC traffic.	block	Block QUIC traffic.					
	Option	Description										
	bypass	Bypass QUIC traffic.										
block	Block QUIC traffic.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
	Option	Description										
	allow	Allow the server certificate.										
	block	Block the session.										
ignore	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td>strict</td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td>disable</td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
	Option	Description										
	enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.										
	strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.										
disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>deep-inspection</td><td>Full SSL inspection.</td></tr></table>	Option	Description	disable	Disable.	deep-inspection	Full SSL inspection.					
	Option	Description										
	disable	Disable.										
deep-inspection	Full SSL inspection.											
udp-not-quic	Action to be taken when matched UDP packet is not QUIC.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Bypass the session when UDP packet is not QUIC.</td></tr><tr><td>block</td><td>Block the session when UDP packet is not QUIC.</td></tr></table>	Option	Description	allow	Bypass the session when UDP packet is not QUIC.	block	Block the session when UDP packet is not QUIC.					
	Option	Description										
	allow	Bypass the session when UDP packet is not QUIC.										
block	Block the session when UDP packet is not QUIC.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option	Description		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	Option	Description		
	<i>allow</i>	Bypass the session when the version is not supported.		
	<i>block</i>	Block the session when the version is not supported.		
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		

config ech-outer-sni

Parameter	Description	Type	Size	Default
name	ClientHelloOuter SNI name.	string	Maximum length: 79	
sni	ClientHelloOuter SNI to be blocked.	string	Maximum length: 255	

config ftps

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Parameter	Description	Type	Size	Default
	Option Description			
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option Description			
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
client-certificate	Action based on received client certificate.	option	-	bypass
	Option Description			
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option Description			
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
min-allowed-ssl-version	Minimum SSL version to be allowed. Flow-based inspection does not support SSL version control.	option	-	tls-1.1
	Option Description			
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.					
	Option	Description										
	<i>tls-1.2</i>	TLS 1.2.										
<i>tls-1.3</i>	TLS 1.3.											
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535									
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
	Option	Description										
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.										
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.										
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
	Option	Description										
	<i>disable</i>	Disable.										
<i>deep-inspection</i>	Full SSL inspection.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option	Description		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	Option	Description		
	<i>allow</i>	Bypass the session when the version is not supported.		
	<i>block</i>	Block the session when the version is not supported.		
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		

config https

Parameter	Description	Type	Size	Default
cert-probe-failure	Action based on certificate probe failure.	option	-	allow
	Option	Description		
	<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.		
	<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
client-certificate	Action based on received client certificate.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
encrypted-client-hello	Block/allow session based on existence of encrypted-client-hello.	option	-	block
	Option	Description		
	<i>allow</i>	Pass the session when encrypted-client-hello exists.		
	<i>block</i>	Block the session when encrypted-client-hello exists.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
min-allowed-ssl-version	Minimum SSL version to be allowed. Flow-based inspection does not support SSL version control.	option	-	tls-1.1

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.			
	Option	Description														
	ssl-3.0	SSL 3.0.														
	tls-1.0	TLS 1.0.														
	tls-1.1	TLS 1.1.														
	tls-1.2	TLS 1.2.														
tls-1.3	TLS 1.3.															
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535													
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.									
	Option	Description														
	enable	Enable setting.														
disable	Disable setting.															
quic	QUIC inspection status (default = inspect).	option	-	inspect												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>inspect</td><td>Inspect QUIC traffic.</td></tr><tr><td>bypass</td><td>Bypass QUIC traffic.</td></tr><tr><td>block</td><td>Block QUIC traffic.</td></tr></table>	Option	Description	inspect	Inspect QUIC traffic.	bypass	Bypass QUIC traffic.	block	Block QUIC traffic.							
	Option	Description														
	inspect	Inspect QUIC traffic.														
	bypass	Bypass QUIC traffic.														
block	Block QUIC traffic.															
revoked-server-cert	Action based on server certificate is revoked.	option	-	block												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.							
	Option	Description														
	allow	Allow the server certificate.														
	block	Block the session.														
ignore	Re-sign the server certificate as trusted.															
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable												

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
	Option	Description										
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.										
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.										
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>certificate-inspection</i></td><td>Inspect SSL handshake only.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>certificate-inspection</i>	Inspect SSL handshake only.	<i>deep-inspection</i>	Full SSL inspection.			
	Option	Description										
	<i>disable</i>	Disable.										
	<i>certificate-inspection</i>	Inspect SSL handshake only.										
<i>deep-inspection</i>	Full SSL inspection.											
udp-not-quic	Action to be taken when matched UDP packet is not QUIC.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when UDP packet is not QUIC.</td></tr><tr><td><i>block</i></td><td>Block the session when UDP packet is not QUIC.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when UDP packet is not QUIC.	<i>block</i>	Block the session when UDP packet is not QUIC.					
	Option	Description										
	<i>allow</i>	Bypass the session when UDP packet is not QUIC.										
<i>block</i>	Block the session when UDP packet is not QUIC.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the cipher is not supported.										
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the negotiation is not supported.										
<i>block</i>	Block the session when the negotiation is not supported.											

Parameter	Description	Type	Size	Default								
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the version is not supported.											
<i>block</i>	Block the session when the version is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config imaps

Parameter	Description	Type	Size	Default								
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
client-certificate	Action based on received client certificate.	option	-	inspect								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.							
Option	Description											
<i>bypass</i>	Bypass the session.											

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.					
	Option	Description										
	<i>inspect</i>	Inspect the session.										
<i>block</i>	Block the session.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.							
	Option	Description										
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
	Option	Description								
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.								
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.									
status	Configure protocol inspection status.	option	-	deep-inspection						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
	Option	Description								
	<i>disable</i>	Disable.								
<i>deep-inspection</i>	Full SSL inspection.									
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.			
	Option	Description								
	<i>allow</i>	Bypass the session when the cipher is not supported.								
<i>block</i>	Block the session when the cipher is not supported.									
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.			
	Option	Description								
	<i>allow</i>	Bypass the session when the negotiation is not supported.								
<i>block</i>	Block the session when the negotiation is not supported.									
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.			
	Option	Description								
	<i>allow</i>	Bypass the session when the version is not supported.								
<i>block</i>	Block the session when the version is not supported.									
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.					
	Option	Description								
<i>allow</i>	Allow the server certificate.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		

config pop3s

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
client-certificate	Action based on received client certificate.	option	-	inspect
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		

Parameter	Description	Type	Size	Default								
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
Option	Description											
enable	Enable setting.											
disable	Disable setting.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td>strict</td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td>disable</td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>deep-inspection</td><td>Full SSL inspection.</td></tr></table>	Option	Description	disable	Disable.	deep-inspection	Full SSL inspection.					
Option	Description											
disable	Disable.											
deep-inspection	Full SSL inspection.											

Parameter	Description	Type	Size	Default								
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the version is not supported.											
<i>block</i>	Block the session when the version is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config smtps

Parameter	Description	Type	Size	Default								
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

Parameter	Description	Type	Size	Default								
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
client-certificate	Action based on received client certificate.	option	-	inspect								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
Option	Description											
enable	Enable setting.											
disable	Disable setting.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
	Option	Description										
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.										
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.										
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
	Option	Description										
	<i>disable</i>	Disable.										
<i>deep-inspection</i>	Full SSL inspection.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the cipher is not supported.										
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the negotiation is not supported.										
<i>block</i>	Block the session when the negotiation is not supported.											

Parameter	Description	Type	Size	Default								
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the version is not supported.											
<i>block</i>	Block the session when the version is not supported.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

config ssh

Parameter	Description	Type	Size	Default						
inspect-all	Level of SSL inspection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>deep-inspection</td><td>Full SSL inspection.</td></tr></table>				Option	Description	disable	Disable.	deep-inspection	Full SSL inspection.
	Option	Description								
	disable	Disable.								
deep-inspection	Full SSL inspection.									
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535							
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-	compatible						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.		
	<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.		
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SSH tunnel policy check.		
	<i>enable</i>	Enable SSH tunnel policy check.		
status	Configure protocol inspection status.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
unsupported-version	Action based on SSH version being unsupported.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>block</i>	Block the session.		

config ssl

Parameter	Description	Type	Size	Default
cert-probe-failure	Action based on certificate probe failure.	option	-	allow
	Option	Description		
	<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.		
	<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
client-certificate	Action based on received client certificate.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
encrypted-client-hello	Block/allow session based on existence of encrypted-client-hello.	option	-	block
	Option	Description		
	<i>allow</i>	Pass the session when encrypted-client-hello exists.		
	<i>block</i>	Block the session when encrypted-client-hello exists.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
inspect-all	Level of SSL inspection.	option	-	disable

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>certificate-inspection</i></td><td>Inspect SSL handshake only.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>certificate-inspection</i>	Inspect SSL handshake only.	<i>deep-inspection</i>	Full SSL inspection.							
	Option	Description														
	<i>disable</i>	Disable.														
	<i>certificate-inspection</i>	Inspect SSL handshake only.														
<i>deep-inspection</i>	Full SSL inspection.															
min-allowed-ssl-version	Minimum SSL version to be allowed. Flow-based inspection does not support SSL version control.	option	-	tls-1.1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description														
	<i>ssl-3.0</i>	SSL 3.0.														
	<i>tls-1.0</i>	TLS 1.0.														
	<i>tls-1.1</i>	TLS 1.1.														
	<i>tls-1.2</i>	TLS 1.2.														
<i>tls-1.3</i>	TLS 1.3.															
revoked-server-cert	Action based on server certificate is revoked.	option	-	block												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.							
	Option	Description														
	<i>allow</i>	Allow the server certificate.														
	<i>block</i>	Block the session.														
<i>ignore</i>	Re-sign the server certificate as trusted.															
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.							
	Option	Description														
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.														
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.														
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.															
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option	Description		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	Option	Description		
	<i>allow</i>	Bypass the session when the version is not supported.		
	<i>block</i>	Block the session when the version is not supported.		
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		

config ssl-exempt

Parameter	Description	Type	Size	Default
address	IPv4 address object.	string	Maximum length: 79	
address6	IPv6 address object.	string	Maximum length: 79	
fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default												
id	ID number.	integer	Minimum value: 0 Maximum value: 512	0												
regex	Exempt servers by regular expression.	string	Maximum length: 255													
type	Type of address object (IPv4 or IPv6) or FortiGuard category.	option	-	fortiguard-category												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fortiguard-category</td><td>FortiGuard category.</td></tr><tr><td>address</td><td>Firewall IPv4 address.</td></tr><tr><td>address6</td><td>Firewall IPv6 address.</td></tr><tr><td>wildcard-fqdn</td><td>Fully Qualified Domain Name with wildcard characters.</td></tr><tr><td>regex</td><td>Regular expression FQDN.</td></tr></table>				Option	Description	fortiguard-category	FortiGuard category.	address	Firewall IPv4 address.	address6	Firewall IPv6 address.	wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.	regex	Regular expression FQDN.
	Option	Description														
	fortiguard-category	FortiGuard category.														
	address	Firewall IPv4 address.														
	address6	Firewall IPv6 address.														
	wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.														
regex	Regular expression FQDN.															
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79													

config ssl-server

Parameter	Description	Type	Size	Default								
ftps-client-certificate	Action based on received client certificate during the FTPS handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
https-client-certificate	Action based on received client certificate during the HTTPS handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											

Parameter	Description	Type	Size	Default								
id	SSL server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
imaps-client-certificate	Action based on received client certificate during the IMAPS handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0								
pop3s-client-certificate	Action based on received client certificate during the POP3S handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
smtps-client-certificate	Action based on received client certificate during the SMTPS handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
ssl-other-client-certificate	Action based on received client certificate during an SSL protocol handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											

config firewall traffic-class

Configure names for shaping classes.

```
config firewall traffic-class
  Description: Configure names for shaping classes.
  edit <class-id>
    set class-name {string}
  next
end
```

config firewall traffic-class

Parameter	Description	Type	Size	Default
class-id	Class ID to be named.	integer	Minimum value: 2 Maximum value: 31	0
class-name	Define the name for this class-id.	string	Maximum length: 35	

config firewall ttl-policy

Configure TTL policies.

```
config firewall ttl-policy
  Description: Configure TTL policies.
  edit <id>
    set action [accept|deny]
    set schedule {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set srcintf {string}
    set status [enable|disable]
    set ttl {user}
  next
end
```


config firewall ttl-policy

Parameter	Description	Type	Size	Default
action	Action to be performed on traffic matching this policy (default = deny).	option	-	deny
	Option	Description		
	accept	Allow traffic matching this policy.		
	deny	Deny or block traffic matching this policy.		
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
schedule	Schedule object from available options.	string	Maximum length: 35	
service <name>	Service object(s) from available options. Separate multiple names with a space. Service name.	string	Maximum length: 79	
srcaddr <name>	Source address object(s) from available options. Separate multiple names with a space. Address name.	string	Maximum length: 79	
srcintf	Source interface name from available interfaces.	string	Maximum length: 35	
status	Enable/disable this TTL policy.	option	-	enable
	Option	Description		
	enable	Enable this TTL policy.		
	disable	Disable this TTL policy.		
ttl	Value/range to match against the packet's Time to Live value (format: ttl[- ttl_high], 1 - 255).	user	Not Specified	

config firewall vendor-mac

Show vendor and the MAC address they have. Read-only.

```
config firewall vendor-mac
  Description: Show vendor and the MAC address they have. Read-only.
  edit <id>
    set mac-number {integer}
    set name {string}
```

```

        set obsolete {integer}
    next
end

```

config firewall vendor-mac

Parameter	Description	Type	Size	Default
id	Vendor ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
mac-number	Total number of MAC addresses. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
name	Vendor name. Read-only.	string	Maximum length: 63	
obsolete	Indicates whether the Vendor ID can be used. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	0

config firewall vip

Configure virtual IP for IPv4.

```

config firewall vip
    Description: Configure virtual IP for IPv4.
    edit <name>
        set add-nat46-route [disable|enable]
        set arp-reply [disable|enable]
        set client-cert [disable|enable]
        set color {integer}
        set comment {var-string}
        set dns-mapping-ttl {integer}
        set empty-cert-action [accept|block|...]
        set extaddr <name1>, <name2>, ...
        set extintf {string}
        set extip {user}
        set extport {user}
        set gratuitous-arp-interval {integer}
        set gslb-domain-name {string}
        set gslb-hostname {string}
    config gslb-public-ips
        Description: Publicly accessible IP addresses for the FortiGSLB service.
        edit <index>

```

```

        set ip {ipv4-address-any}
    next
end
set h2-support [enable|disable]
set h3-support [enable|disable]
set http-cookie-age {integer}
set http-cookie-domain {string}
set http-cookie-domain-from-host [disable|enable]
set http-cookie-generation {integer}
set http-cookie-path {string}
set http-cookie-share [disable|same-ip]
set http-ip-header [enable|disable]
set http-ip-header-name {string}
set http-multiplex [enable|disable]
set http-multiplex-max-concurrent-request {integer}
set http-multiplex-max-request {integer}
set http-multiplex-ttl {integer}
set http-redirect [enable|disable]
set https-cookie-secure [disable|enable]
set id {integer}
set ipv6-mappedip {user}
set ipv6-mappedport {user}
set ldb-method [static|round-robin|...]
set mapped-addr {string}
set mappedip <range1>, <range2>, ...
set mappedport {user}
set max-embryonic-connections {integer}
set monitor <name1>, <name2>, ...
set nat-source-vip [disable|enable]
set nat44 [disable|enable]
set nat46 [disable|enable]
set one-click-gslb-server [disable|enable]
set outlook-web-access [disable|enable]
set persistence [none|http-cookie|...]
set portforward [disable|enable]
set portmapping-type [1-to-1|m-to-n]
set protocol [tcp|udp|...]
config quic
    Description: QUIC setting.
    set ack-delay-exponent {integer}
    set active-connection-id-limit {integer}
    set active-migration [enable|disable]
    set grease-quic-bit [enable|disable]
    set max-ack-delay {integer}
    set max-datagram-frame-size {integer}
    set max-idle-timeout {integer}
    set max-udp-payload-size {integer}
end
config realservers
    Description: Select the real servers that this server load balancing VIP will
    distribute traffic to.
    edit <id>

```

```

        set address {string}
        set client-ip {user}
        set healthcheck [disable|enable|...]
        set holddown-interval {integer}
        set http-host {string}
        set ip {user}
        set max-connections {integer}
        set monitor <name1>, <name2>, ...
        set port {integer}
        set status [active|standby|...]
        set translate-host [enable|disable]
        set type [ip|address]
        set verify-cert [enable|disable]
        set weight {integer}
    next
end
set server-type [http|https|...]
set service <name1>, <name2>, ...
set src-filter <range1>, <range2>, ...
set src-vip-filter [disable|enable]
set srcintf-filter <interface-name1>, <interface-name2>, ...
set ssl-accept-ffdhe-groups [enable|disable]
set ssl-algorithm [high|medium|...]
set ssl-certificate <name1>, <name2>, ...
config ssl-cipher-suites
    Description: SSL/TLS cipher suites acceptable from a client, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-client-fallback [disable|enable]
set ssl-client-rekey-count {integer}
set ssl-client-renegotiation [allow|deny|...]
set ssl-client-session-state-max {integer}
set ssl-client-session-state-timeout {integer}
set ssl-client-session-state-type [disable|time|...]
set ssl-dh-bits [768|1024|...]
set ssl-hpkip [disable|enable|...]
set ssl-hpkip-age {integer}
set ssl-hpkip-backup {string}
set ssl-hpkip-include-subdomains [disable|enable]
set ssl-hpkip-primary {string}
set ssl-hpkip-report-uri {var-string}
set ssl-hsts [disable|enable]
set ssl-hsts-age {integer}
set ssl-hsts-include-subdomains [disable|enable]
set ssl-http-location-conversion [enable|disable]
set ssl-http-match-host [enable|disable]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-mode [half|full]

```

```

set ssl-pfs [require|deny|...]
set ssl-send-empty-frags [enable|disable]
set ssl-server-algorithm [high|medium|...]
config ssl-server-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-server-max-version [ssl-3.0|tls-1.0|...]
set ssl-server-min-version [ssl-3.0|tls-1.0|...]
set ssl-server-renegotiation [enable|disable]
set ssl-server-session-state-max {integer}
set ssl-server-session-state-timeout {integer}
set ssl-server-session-state-type [disable|time|...]
set status [disable|enable]
set type [static-nat|load-balance|...]
set user-agent-detect [disable|enable]
set uuid {uuid}
set weblogic-server [disable|enable]
set websphere-server [disable|enable]
next
end

```

config firewall vip

Parameter	Description	Type	Size	Default						
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable adding NAT46 route.</td></tr><tr><td><i>enable</i></td><td>Enable adding NAT46 route.</td></tr></table>	Option	Description	<i>disable</i>	Disable adding NAT46 route.	<i>enable</i>	Enable adding NAT46 route.			
Option	Description									
<i>disable</i>	Disable adding NAT46 route.									
<i>enable</i>	Enable adding NAT46 route.									
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable ARP reply.</td></tr><tr><td><i>enable</i></td><td>Enable ARP reply.</td></tr></table>	Option	Description	<i>disable</i>	Disable ARP reply.	<i>enable</i>	Enable ARP reply.			
Option	Description									
<i>disable</i>	Disable ARP reply.									
<i>enable</i>	Enable ARP reply.									
client-cert	Enable/disable requesting client certificate.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable client certificate request.		
	<i>enable</i>	Enable client certificate request.		
color	Color of icon on the GUI.	integer	Minimum value: 0 0 Maximum value: 32	
comment	Comment.	var-string	Maximum length: 255	
dns-mapping-ttl	DNS mapping TTL (Set to zero to use TTL in DNS response, default = 0).	integer	Minimum value: 0 0 Maximum value: 604800	
empty-cert-action	Action for an empty client certificate.	option	-	block
	Option	Description		
	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.		
	<i>block</i>	Block the SSL handshake if the client certificate is empty.		
	<i>accept-unmanageable</i>	Accept the SSL handshake only if the end-point is unmanageable.		
extaddr <name>	External FQDN address name. Address name.	string	Maximum length: 79	
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35	
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified	
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified	
gratuitous-arp-interval	Enable to have the VIP send gratuitous ARPs. 0=disabled. Set from 5 up to 8640000 seconds to enable.	integer	Minimum value: 0 5 Maximum value: 8640000	

Parameter	Description	Type	Size	Default						
gslb-domain-name	Domain to use when integrating with FortiGSLB.	string	Maximum length: 255							
gslb-hostname	Hostname to use within the configured FortiGSLB domain.	string	Maximum length: 35							
h2-support	Enable/disable HTTP2 support (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP2 support.</td></tr><tr><td>disable</td><td>Disable HTTP2 support.</td></tr></table>				Option	Description	enable	Enable HTTP2 support.	disable	Disable HTTP2 support.
Option	Description									
enable	Enable HTTP2 support.									
disable	Disable HTTP2 support.									
h3-support	Enable/disable HTTP3/QUIC support (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP3/QUIC support.</td></tr><tr><td>disable</td><td>Disable HTTP3/QUIC support.</td></tr></table>				Option	Description	enable	Enable HTTP3/QUIC support.	disable	Disable HTTP3/QUIC support.
Option	Description									
enable	Enable HTTP3/QUIC support.									
disable	Disable HTTP3/QUIC support.									
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td>enable</td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>				Option	Description	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).	enable	Enable use of HTTP cookie domain from host field in HTTP.
Option	Description									
disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).									
enable	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
http-cookie-share	Control sharing of cookies across virtual servers. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Only allow HTTP cookie to match this virtual server.</td></tr><tr><td>same-ip</td><td>Allow HTTP cookie to match any virtual server with same IP.</td></tr></table>	Option	Description	disable	Only allow HTTP cookie to match this virtual server.	same-ip	Allow HTTP cookie to match any virtual server with same IP.			
Option	Description									
disable	Only allow HTTP cookie to match this virtual server.									
same-ip	Allow HTTP cookie to match any virtual server with same IP.									
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the X-Forwarded-For HTTP header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable adding HTTP header.</td></tr><tr><td>disable</td><td>Disable adding HTTP header.</td></tr></table>	Option	Description	enable	Enable adding HTTP header.	disable	Disable adding HTTP header.			
Option	Description									
enable	Enable adding HTTP header.									
disable	Disable adding HTTP header.									
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35							
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP session multiplexing.</td></tr><tr><td>disable</td><td>Disable HTTP session multiplexing.</td></tr></table>	Option	Description	enable	Enable HTTP session multiplexing.	disable	Disable HTTP session multiplexing.			
Option	Description									
enable	Enable HTTP session multiplexing.									
disable	Disable HTTP session multiplexing.									
http-multiplex-max-concurrent-request	Maximum number of concurrent requests that a multiplex server can handle (default = unlimited).	integer	Minimum value: 0 0 Maximum value: 2147483647							
http-multiplex-max-request	Maximum number of requests that a multiplex server can handle before disconnecting sessions (default = unlimited).	integer	Minimum value: 0 0 Maximum value: 2147483647							
http-multiplex-ttl	Time-to-live for idle connections to servers.	integer	Minimum value: 0 0 Maximum value: 2147483647	15						

Parameter	Description	Type	Size	Default																
http-redirect	Enable/disable redirection of HTTP to HTTPS.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redirection of HTTP to HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable redirection of HTTP to HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable redirection of HTTP to HTTPS.	<i>disable</i>	Disable redirection of HTTP to HTTPS.													
Option	Description																			
<i>enable</i>	Enable redirection of HTTP to HTTPS.																			
<i>disable</i>	Disable redirection of HTTP to HTTPS.																			
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td><i>enable</i></td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>	Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.													
Option	Description																			
<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.																			
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.																			
id	Custom defined ID.	integer	Minimum value: 0 0 Maximum value: 65535																	
ipv6-mappedip	Range of mapped IPv6 addresses. Specify the start IPv6 address followed by a space and the end IPv6 address.	user	Not Specified																	
ipv6-mappedport	IPv6 port number range on the destination network to which the external port number range is mapped.	user	Not Specified																	
ldb-method	Method used to distribute sessions to real servers.	option	-	static																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute to server based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute to server based round robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute to server based on weight.</td></tr><tr><td><i>least-session</i></td><td>Distribute to server with lowest session count.</td></tr><tr><td><i>least-rtt</i></td><td>Distribute to server with lowest Round-Trip-Time.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	<i>static</i>	Distribute to server based on source IP.	<i>round-robin</i>	Distribute to server based round robin order.	<i>weighted</i>	Distribute to server based on weight.	<i>least-session</i>	Distribute to server with lowest session count.	<i>least-rtt</i>	Distribute to server with lowest Round-Trip-Time.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.			
Option	Description																			
<i>static</i>	Distribute to server based on source IP.																			
<i>round-robin</i>	Distribute to server based round robin order.																			
<i>weighted</i>	Distribute to server based on weight.																			
<i>least-session</i>	Distribute to server with lowest session count.																			
<i>least-rtt</i>	Distribute to server with lowest Round-Trip-Time.																			
<i>first-alive</i>	Distribute to the first server that is alive.																			
<i>http-host</i>	Distribute to server based on host field in HTTP header.																			

Parameter	Description	Type	Size	Default						
mapped-addr	Mapped FQDN address name.	string	Maximum length: 79							
mappedip <range>	IP address or address range on the destination network to which the external IP address is mapped. Mapped IP range.	string	Maximum length: 79							
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified							
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 1000 0 Maximum value: 100000							
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79							
name	Virtual IP name.	string	Maximum length: 79							
nat-source-vip	Enable/disable forcing the source NAT mapped IP to the external IP for all traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.</td></tr><tr><td>enable</td><td>Force the source NAT mapped IP to the external IP for all traffic.</td></tr></table>	Option	Description	disable	Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.	enable	Force the source NAT mapped IP to the external IP for all traffic.			
Option	Description									
disable	Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.									
enable	Force the source NAT mapped IP to the external IP for all traffic.									
nat44	Enable/disable NAT44.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NAT44.</td></tr><tr><td>enable</td><td>Enable NAT44.</td></tr></table>	Option	Description	disable	Disable NAT44.	enable	Enable NAT44.			
Option	Description									
disable	Disable NAT44.									
enable	Enable NAT44.									
nat46	Enable/disable NAT46.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NAT46.</td></tr><tr><td>enable</td><td>Enable NAT46.</td></tr></table>	Option	Description	disable	Disable NAT46.	enable	Enable NAT46.			
Option	Description									
disable	Disable NAT46.									
enable	Enable NAT46.									

Parameter	Description	Type	Size	Default								
one-click-gslb-server	Enable/disable one click GSLB server integration with FortiGSLB.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable integration with FortiGSLB.</td></tr><tr><td><i>enable</i></td><td>Enable integration with FortiGSLB.</td></tr></table>	Option	Description	<i>disable</i>	Disable integration with FortiGSLB.	<i>enable</i>	Enable integration with FortiGSLB.					
Option	Description											
<i>disable</i>	Disable integration with FortiGSLB.											
<i>enable</i>	Enable integration with FortiGSLB.											
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Outlook Web Access support.</td></tr><tr><td><i>enable</i></td><td>Enable Outlook Web Access support.</td></tr></table>	Option	Description	<i>disable</i>	Disable Outlook Web Access support.	<i>enable</i>	Enable Outlook Web Access support.					
Option	Description											
<i>disable</i>	Disable Outlook Web Access support.											
<i>enable</i>	Enable Outlook Web Access support.											
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr><tr><td><i>ssl-session-id</i></td><td>SSL session ID.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.	<i>ssl-session-id</i>	SSL session ID.			
Option	Description											
<i>none</i>	None.											
<i>http-cookie</i>	HTTP cookie.											
<i>ssl-session-id</i>	SSL session ID.											
portforward	Enable/disable port forwarding.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable port forward.</td></tr><tr><td><i>enable</i></td><td>Enable port forward.</td></tr></table>	Option	Description	<i>disable</i>	Disable port forward.	<i>enable</i>	Enable port forward.					
Option	Description											
<i>disable</i>	Disable port forward.											
<i>enable</i>	Enable port forward.											
portmapping-type	Port mapping type.	option	-	1-to-1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1-to-1</i></td><td>One to one.</td></tr><tr><td><i>m-to-n</i></td><td>Many to many.</td></tr></table>	Option	Description	<i>1-to-1</i>	One to one.	<i>m-to-n</i>	Many to many.					
Option	Description											
<i>1-to-1</i>	One to one.											
<i>m-to-n</i>	Many to many.											
protocol	Protocol to use when forwarding packets.	option	-	tcp								

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>sctp</i></td><td>SCTP.</td></tr><tr><td><i>icmp</i></td><td>ICMP.</td></tr></table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>sctp</i>	SCTP.	<i>icmp</i>	ICMP.													
	Option	Description																						
	<i>tcp</i>	TCP.																						
	<i>udp</i>	UDP.																						
	<i>sctp</i>	SCTP.																						
<i>icmp</i>	ICMP.																							
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>ssl</i></td><td>SSL.</td></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>ip</i></td><td>IP.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.	<i>imaps</i>	IMAPS.	<i>pop3s</i>	POP3S.	<i>smtps</i>	SMTPS.	<i>ssl</i>	SSL.	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>ip</i>	IP.			
	Option	Description																						
	<i>http</i>	HTTP.																						
	<i>https</i>	HTTPS.																						
	<i>imaps</i>	IMAPS.																						
	<i>pop3s</i>	POP3S.																						
	<i>smtps</i>	SMTPS.																						
	<i>ssl</i>	SSL.																						
	<i>tcp</i>	TCP.																						
<i>udp</i>	UDP.																							
<i>ip</i>	IP.																							
service <name>	Service name. Service name.	string	Maximum length: 79																					
src-filter <range>	Source address filter. Each address must be either an IP/subnet (x.x.x.x/n) or a range (x.x.x.x-y.y.y.y). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79																					
src-vip-filter	Enable/disable use of 'src-filter' to match destinations for the reverse SNAT rule.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Match any destination for the reverse SNAT rule.</td></tr><tr><td><i>enable</i></td><td>Match only destinations in 'src-filter' for the reverse SNAT rule.</td></tr></table>	Option	Description	<i>disable</i>	Match any destination for the reverse SNAT rule.	<i>enable</i>	Match only destinations in 'src-filter' for the reverse SNAT rule.																	
	Option	Description																						
	<i>disable</i>	Match any destination for the reverse SNAT rule.																						
<i>enable</i>	Match only destinations in 'src-filter' for the reverse SNAT rule.																							

Parameter	Description	Type	Size	Default										
srcintf-filter <interface-name>	Interfaces to which the VIP applies. Separate the names with spaces. Interface name.	string	Maximum length: 79											
ssl-accept- ffdhe-groups	Enable/disable FFDHE cipher suite for SSL key exchange.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Accept FFDHE groups.</td></tr><tr><td>disable</td><td>Do not accept FFDHE groups.</td></tr></table>	Option	Description	enable	Accept FFDHE groups.	disable	Do not accept FFDHE groups.							
Option	Description													
enable	Accept FFDHE groups.													
disable	Do not accept FFDHE groups.													
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-	high										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr><tr><td>custom</td><td>Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.</td></tr></table>	Option	Description	high	High encryption. Allow only AES and ChaCha.	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	custom	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.			
Option	Description													
high	High encryption. Allow only AES and ChaCha.													
medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.													
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.													
custom	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.													
ssl-certificate <name>	Name of the certificate to use for SSL handshake. Certificate list.	string	Maximum length: 79											
ssl-client- fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>enable</td><td>Enable.</td></tr></table>	Option	Description	disable	Disable.	enable	Enable.							
Option	Description													
disable	Disable.													
enable	Enable.													
ssl-client- rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 0 200 Maximum value: 1048576											
ssl-client- renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-	secure										

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow a SSL client to renegotiate.</td></tr><tr><td><i>deny</i></td><td>Abort any client initiated SSL re-negotiation attempt.</td></tr><tr><td><i>secure</i></td><td>Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.</td></tr></table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.	<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.									
	Option	Description																
	<i>allow</i>	Allow a SSL client to renegotiate.																
	<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.																
<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.																	
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1000 1 Maximum value: 10000															
ssl-client-session-state-timeout	Number of minutes to keep client to FortiGate SSL session state.	integer	Minimum value: 30 1 Maximum value: 14400															
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-	both														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not keep session states.</td></tr><tr><td><i>time</i></td><td>Expire session states after this many minutes.</td></tr><tr><td><i>count</i></td><td>Expire session states when this maximum is reached.</td></tr><tr><td><i>both</i></td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.							
	Option	Description																
	<i>disable</i>	Do not keep session states.																
	<i>time</i>	Expire session states after this many minutes.																
	<i>count</i>	Expire session states when this maximum is reached.																
<i>both</i>	Expire session states based on time or count, whichever occurs first.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td><i>3072</i></td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td><i>4096</i></td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.			
	Option	Description																
	<i>768</i>	768-bit Diffie-Hellman prime.																
	<i>1024</i>	1024-bit Diffie-Hellman prime.																
	<i>1536</i>	1536-bit Diffie-Hellman prime.																
	<i>2048</i>	2048-bit Diffie-Hellman prime.																
	<i>3072</i>	3072-bit Diffie-Hellman prime.																
<i>4096</i>	4096-bit Diffie-Hellman prime.																	
ssl-hpkip	Enable/disable including HPKP header in response.	option	-	disable														

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a HPKP header to each HTTP response.</td></tr><tr><td>enable</td><td>Add a HPKP header to each a HTTP response.</td></tr><tr><td>report-only</td><td>Add a HPKP Report-Only header to each HTTP response.</td></tr></table>	Option	Description	disable	Do not add a HPKP header to each HTTP response.	enable	Add a HPKP header to each a HTTP response.	report-only	Add a HPKP Report-Only header to each HTTP response.			
	Option	Description										
	disable	Do not add a HPKP header to each HTTP response.										
	enable	Add a HPKP header to each a HTTP response.										
report-only	Add a HPKP Report-Only header to each HTTP response.											
ssl-hpkp-age	Number of seconds the client should honor the HPKP setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000								
ssl-hpkp-backup	Certificate to generate backup HPKP pin from.	string	Maximum length: 79									
ssl-hpkp-include-subdomains	Indicate that HPKP header applies to all subdomains.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>HPKP header does not apply to subdomains.</td></tr><tr><td>enable</td><td>HPKP header applies to subdomains.</td></tr></table>	Option	Description	disable	HPKP header does not apply to subdomains.	enable	HPKP header applies to subdomains.					
	Option	Description										
	disable	HPKP header does not apply to subdomains.										
enable	HPKP header applies to subdomains.											
ssl-hpkp-primary	Certificate to generate primary HPKP pin from.	string	Maximum length: 79									
ssl-hpkp-report-uri	URL to report HPKP violations to.	var-string	Maximum length: 255									
ssl-hsts	Enable/disable including HSTS header in response.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a HSTS header to each a HTTP response.</td></tr><tr><td>enable</td><td>Add a HSTS header to each HTTP response.</td></tr></table>	Option	Description	disable	Do not add a HSTS header to each a HTTP response.	enable	Add a HSTS header to each HTTP response.					
	Option	Description										
	disable	Do not add a HSTS header to each a HTTP response.										
enable	Add a HSTS header to each HTTP response.											
ssl-hsts-age	Number of seconds the client should honor the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000								
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-	disable								

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>HSTS header does not apply to subdomains.</td></tr><tr><td><i>enable</i></td><td>HSTS header applies to subdomains.</td></tr></table>	Option	Description	<i>disable</i>	HSTS header does not apply to subdomains.	<i>enable</i>	HSTS header applies to subdomains.									
	Option	Description														
	<i>disable</i>	HSTS header does not apply to subdomains.														
<i>enable</i>	HSTS header applies to subdomains.															
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP location conversion.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP location conversion.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP location conversion.	<i>disable</i>	Disable HTTP location conversion.									
	Option	Description														
	<i>enable</i>	Enable HTTP location conversion.														
<i>disable</i>	Disable HTTP location conversion.															
ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Match HTTP host in response header.</td></tr><tr><td><i>disable</i></td><td>Do not match HTTP host.</td></tr></table>	Option	Description	<i>enable</i>	Match HTTP host in response header.	<i>disable</i>	Do not match HTTP host.									
	Option	Description														
	<i>enable</i>	Match HTTP host in response header.														
<i>disable</i>	Do not match HTTP host.															
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.3												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description														
	<i>ssl-3.0</i>	SSL 3.0.														
	<i>tls-1.0</i>	TLS 1.0.														
	<i>tls-1.1</i>	TLS 1.1.														
	<i>tls-1.2</i>	TLS 1.2.														
<i>tls-1.3</i>	TLS 1.3.															
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-	tls-1.1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description														
	<i>ssl-3.0</i>	SSL 3.0.														
	<i>tls-1.0</i>	TLS 1.0.														
	<i>tls-1.1</i>	TLS 1.1.														
	<i>tls-1.2</i>	TLS 1.2.														
<i>tls-1.3</i>	TLS 1.3.															

Parameter	Description	Type	Size	Default								
ssl-mode	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-	half								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>half</td><td>Client to FortiGate SSL.</td></tr><tr><td>full</td><td>Client to FortiGate and FortiGate to Server SSL.</td></tr></table>	Option	Description	half	Client to FortiGate SSL.	full	Client to FortiGate and FortiGate to Server SSL.					
Option	Description											
half	Client to FortiGate SSL.											
full	Client to FortiGate and FortiGate to Server SSL.											
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-	require								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>require</td><td>Allow only Diffie-Hellman cipher-suites, so PFS is applied.</td></tr><tr><td>deny</td><td>Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</td></tr><tr><td>allow</td><td>Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</td></tr></table>	Option	Description	require	Allow only Diffie-Hellman cipher-suites, so PFS is applied.	deny	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.	allow	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.			
Option	Description											
require	Allow only Diffie-Hellman cipher-suites, so PFS is applied.											
deny	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.											
allow	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.											
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Send empty fragments.</td></tr><tr><td>disable</td><td>Do not send empty fragments.</td></tr></table>	Option	Description	enable	Send empty fragments.	disable	Do not send empty fragments.					
Option	Description											
enable	Send empty fragments.											
disable	Do not send empty fragments.											
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	client								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	high	High encryption. Allow only AES and ChaCha.	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.			
Option	Description											
high	High encryption. Allow only AES and ChaCha.											
medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.											
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>custom</i></td><td>Custom encryption. Use <code>ssl-server-cipher-suites</code> to select the cipher suites that are allowed.</td></tr><tr><td><i>client</i></td><td>Use the same encryption algorithms for both client and server sessions.</td></tr></table>	Option	Description	<i>custom</i>	Custom encryption. Use <code>ssl-server-cipher-suites</code> to select the cipher suites that are allowed.	<i>client</i>	Use the same encryption algorithms for both client and server sessions.											
	Option	Description																
	<i>custom</i>	Custom encryption. Use <code>ssl-server-cipher-suites</code> to select the cipher suites that are allowed.																
<i>client</i>	Use the same encryption algorithms for both client and server sessions.																	
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr><tr><td><i>client</i></td><td>Use same value as client configuration.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
	Option	Description																
	<i>ssl-3.0</i>	SSL 3.0.																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
	<i>tls-1.3</i>	TLS 1.3.																
<i>client</i>	Use same value as client configuration.																	
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr><tr><td><i>client</i></td><td>Use same value as client configuration.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
	Option	Description																
	<i>ssl-3.0</i>	SSL 3.0.																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
	<i>tls-1.3</i>	TLS 1.3.																
<i>client</i>	Use same value as client configuration.																	
ssl-server-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable secure renegotiation.</td></tr><tr><td><i>disable</i></td><td>Disable secure renegotiation.</td></tr></table>	Option	Description	<i>enable</i>	Enable secure renegotiation.	<i>disable</i>	Disable secure renegotiation.											
	Option	Description																
	<i>enable</i>	Enable secure renegotiation.																
<i>disable</i>	Disable secure renegotiation.																	

Parameter	Description	Type	Size	Default														
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	100														
ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60														
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-	both														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not keep session states.</td></tr><tr><td>time</td><td>Expire session states after this many minutes.</td></tr><tr><td>count</td><td>Expire session states when this maximum is reached.</td></tr><tr><td>both</td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>				Option	Description	disable	Do not keep session states.	time	Expire session states after this many minutes.	count	Expire session states when this maximum is reached.	both	Expire session states based on time or count, whichever occurs first.				
Option	Description																	
disable	Do not keep session states.																	
time	Expire session states after this many minutes.																	
count	Expire session states when this maximum is reached.																	
both	Expire session states based on time or count, whichever occurs first.																	
status	Enable/disable VIP.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable the VIP.</td></tr><tr><td>enable</td><td>Enable the VIP.</td></tr></table>				Option	Description	disable	Disable the VIP.	enable	Enable the VIP.								
Option	Description																	
disable	Disable the VIP.																	
enable	Enable the VIP.																	
type	Configure a static NAT, load balance, server load balance, access proxy, DNS translation, or FQDN VIP.	option	-	static-nat														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static-nat</td><td>Static NAT.</td></tr><tr><td>load-balance</td><td>Load balance.</td></tr><tr><td>server-load-balance</td><td>Server load balance.</td></tr><tr><td>dns-translation</td><td>DNS translation.</td></tr><tr><td>fqdn</td><td>Fully qualified domain name.</td></tr><tr><td>access-proxy</td><td>Access proxy.</td></tr></table>				Option	Description	static-nat	Static NAT.	load-balance	Load balance.	server-load-balance	Server load balance.	dns-translation	DNS translation.	fqdn	Fully qualified domain name.	access-proxy	Access proxy.
Option	Description																	
static-nat	Static NAT.																	
load-balance	Load balance.																	
server-load-balance	Server load balance.																	
dns-translation	DNS translation.																	
fqdn	Fully qualified domain name.																	
access-proxy	Access proxy.																	
user-agent-detect	Enable/disable detecting device type by HTTP user-agent if no client certificate is provided.	option	-	enable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable detecting unknown devices by HTTP user-agent if no client certificate is provided.		
	<i>enable</i>	Enable detecting unknown devices by HTTP user-agent if no client certificate is provided.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.		
	<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.		
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.		
	<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.		

config gslb-public-ips

Parameter	Description	Type	Size	Default
index	Index of this public IP setting.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	The publicly accessible IP address.	ipv4-address-any	Not Specified	0.0.0.0

config quic

Parameter	Description	Type	Size	Default						
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3						
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2						
active-migration	Enable/disable active migration (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable active migration.</td></tr><tr><td><i>disable</i></td><td>Disable active migration.</td></tr></table>	Option	Description	<i>enable</i>	Enable active migration.	<i>disable</i>	Disable active migration.			
Option	Description									
<i>enable</i>	Enable active migration.									
<i>disable</i>	Disable active migration.									
grease-quic-bit	Enable/disable grease QUIC bit (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable grease QUIC bit.</td></tr><tr><td><i>disable</i></td><td>Disable grease QUIC bit.</td></tr></table>	Option	Description	<i>enable</i>	Enable grease QUIC bit.	<i>disable</i>	Disable grease QUIC bit.			
Option	Description									
<i>enable</i>	Enable grease QUIC bit.									
<i>disable</i>	Disable grease QUIC bit.									
max-ack-delay	Maximum ACK delay in milliseconds (1 - 16383, default = 25).	integer	Minimum value: 1 Maximum value: 16383	25						
max-datagram-frame-size	Maximum datagram frame size in bytes (1 - 1500, default = 1500).	integer	Minimum value: 1 Maximum value: 1500	1500						
max-idle-timeout	Maximum idle timeout milliseconds (1 - 60000, default = 30000).	integer	Minimum value: 1 Maximum value: 60000	30000						
max-udp-payload-size	Maximum UDP payload size in bytes (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500						

config realservers

Parameter	Description	Type	Size	Default								
address	Dynamic address of the real server.	string	Maximum length: 79									
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified									
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	vip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable per server health check.</td></tr><tr><td>enable</td><td>Enable per server health check.</td></tr><tr><td>vip</td><td>Use health check defined in VIP.</td></tr></table>	Option	Description	disable	Disable per server health check.	enable	Enable per server health check.	vip	Use health check defined in VIP.			
Option	Description											
disable	Disable per server health check.											
enable	Enable per server health check.											
vip	Use health check defined in VIP.											
holddown-interval	Time in seconds that the system waits before re-activating a previously down active server in the active-standby mode. This is to prevent any flapping issues.	integer	Minimum value: 30 Maximum value: 65535	300								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
ip	IP address of the real server.	user	Not Specified									
max-connections	Max number of active connections that can be directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0								
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79									
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 1 Maximum value: 65535	0								
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Server status active.</td></tr><tr><td><i>standby</i></td><td>Server status standby.</td></tr><tr><td><i>disable</i></td><td>Server status disable.</td></tr></table>	Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.			
	Option	Description										
	<i>active</i>	Server status active.										
	<i>standby</i>	Server status standby.										
<i>disable</i>	Server status disable.											
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable virtual hostname/IP translation.</td></tr><tr><td><i>disable</i></td><td>Disable virtual hostname/IP translation.</td></tr></table>	Option	Description	<i>enable</i>	Enable virtual hostname/IP translation.	<i>disable</i>	Disable virtual hostname/IP translation.					
	Option	Description										
	<i>enable</i>	Enable virtual hostname/IP translation.										
<i>disable</i>	Disable virtual hostname/IP translation.											
type	Type of address.	option	-	ip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>address</i></td><td>Dynamic address object.</td></tr></table>	Option	Description	<i>ip</i>	Standard IPv4 address.	<i>address</i>	Dynamic address object.					
	Option	Description										
	<i>ip</i>	Standard IPv4 address.										
<i>address</i>	Dynamic address object.											
verify-cert	Enable/disable certificate verification of the real server.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable certificate verification.</td></tr><tr><td><i>disable</i></td><td>Disable certificate verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable certificate verification.	<i>disable</i>	Disable certificate verification.					
	Option	Description										
	<i>enable</i>	Enable certificate verification.										
<i>disable</i>	Disable certificate verification.											
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								

config ssl-cipher-suites

Parameter	Description	Type	Size	Default						
cipher	Cipher suite name.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-AES-256-GCM-SHA384.</td></tr></table>	Option	Description	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.			
Option	Description									
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.									
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.									

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr></table>	Option	Description	TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.			
Option	Description																									
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.																									
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																									
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.																									
TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																									
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																									
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																									
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																									
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																									
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																									
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																									

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.</td></tr></table>	Option	Description	TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.			
Option	Description																									
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																									
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																									
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																									
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.																									
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.																									
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.																									
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.																									
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.																									
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.																									
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.																									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.			
Option	Description																									
<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																									
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256.																									

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																								
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																								
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																								
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																								
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																								
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																								
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																								
<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																									
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																									
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295																							

Parameter	Description	Type	Size	Default
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3

Option	Description
ssl-3.0	SSL 3.0.
tls-1.0	TLS 1.0.
tls-1.1	TLS 1.1.
tls-1.2	TLS 1.2.
tls-1.3	TLS 1.3.

config ssl-server-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	

Option	Description
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.
TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.			
Option	Description																									
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																									
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																									
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																									
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																									
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																									

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																				
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																				
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																				
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																				
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																				
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																					
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295																			
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.															
	Option	Description																				
	<i>ssl-3.0</i>	SSL 3.0.																				
<i>tls-1.0</i>	TLS 1.0.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config firewall vip6

Configure virtual IP for IPv6.

```
config firewall vip6
  Description: Configure virtual IP for IPv6.
  edit <name>
    set add-nat64-route [disable|enable]
    set client-cert [disable|enable]
    set color {integer}
    set comment {var-string}
    set embedded-ipv4-address [disable|enable]
    set empty-cert-action [accept|block|...]
    set extip {user}
    set extport {user}
    set h2-support [enable|disable]
    set h3-support [enable|disable]
    set http-cookie-age {integer}
    set http-cookie-domain {string}
    set http-cookie-domain-from-host [disable|enable]
    set http-cookie-generation {integer}
    set http-cookie-path {string}
    set http-cookie-share [disable|same-ip]
    set http-ip-header [enable|disable]
    set http-ip-header-name {string}
    set http-multiplex [enable|disable]
    set http-redirect [enable|disable]
    set https-cookie-secure [disable|enable]
    set id {integer}
    set ipv4-mappedip {user}
    set ipv4-mappedport {user}
    set ldb-method [static|round-robin|...]
    set mappedip {user}
    set mappedport {user}
    set max-embryonic-connections {integer}
    set monitor <name1>, <name2>, ...
    set nat-source-vip [disable|enable]
    set nat64 [disable|enable]
    set nat66 [disable|enable]
    set ndp-reply [disable|enable]
    set outlook-web-access [disable|enable]
```

```

set persistence [none|http-cookie|...]
set portforward [disable|enable]
set protocol [tcp|udp|...]
config quic
    Description: QUIC setting.
    set ack-delay-exponent {integer}
    set active-connection-id-limit {integer}
    set active-migration [enable|disable]
    set grease-quic-bit [enable|disable]
    set max-ack-delay {integer}
    set max-datagram-frame-size {integer}
    set max-idle-timeout {integer}
    set max-udp-payload-size {integer}
end
config realservers
    Description: Select the real servers that this server load balancing VIP will
distribute traffic to.
    edit <id>
        set client-ip {user}
        set healthcheck [disable|enable|...]
        set holddown-interval {integer}
        set http-host {string}
        set ip {user}
        set max-connections {integer}
        set monitor <name1>, <name2>, ...
        set port {integer}
        set status [active|standby|...]
        set translate-host [enable|disable]
        set weight {integer}
    next
end
set server-type [http|https|...]
set src-filter <range1>, <range2>, ...
set src-vip-filter [disable|enable]
set ssl-accept-ffdhe-groups [enable|disable]
set ssl-algorithm [high|medium|...]
set ssl-certificate <name1>, <name2>, ...
config ssl-cipher-suites
    Description: SSL/TLS cipher suites acceptable from a client, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-client-fallback [disable|enable]
set ssl-client-rekey-count {integer}
set ssl-client-renegotiation [allow|deny|...]
set ssl-client-session-state-max {integer}
set ssl-client-session-state-timeout {integer}
set ssl-client-session-state-type [disable|time|...]
set ssl-dh-bits [768|1024|...]
set ssl-hpkip [disable|enable|...]

```



```

set ssl-hpkp-age {integer}
set ssl-hpkp-backup {string}
set ssl-hpkp-include-subdomains [disable|enable]
set ssl-hpkp-primary {string}
set ssl-hpkp-report-uri {var-string}
set ssl-hsts [disable|enable]
set ssl-hsts-age {integer}
set ssl-hsts-include-subdomains [disable|enable]
set ssl-http-location-conversion [enable|disable]
set ssl-http-match-host [enable|disable]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-mode [half|full]
set ssl-pfs [require|deny|...]
set ssl-send-empty-frags [enable|disable]
set ssl-server-algorithm [high|medium|...]
config ssl-server-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-server-max-version [ssl-3.0|tls-1.0|...]
set ssl-server-min-version [ssl-3.0|tls-1.0|...]
set ssl-server-renegotiation [enable|disable]
set ssl-server-session-state-max {integer}
set ssl-server-session-state-timeout {integer}
set ssl-server-session-state-type [disable|time|...]
set type [static-nat|server-load-balance|...]
set user-agent-detect [disable|enable]
set uuid {uuid}
set weblogic-server [disable|enable]
set websphere-server [disable|enable]
next
end

```

config firewall vip6

Parameter	Description	Type	Size	Default						
add-nat64-route	Enable/disable adding NAT64 route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable adding NAT64 route.</td></tr><tr><td><i>enable</i></td><td>Enable adding NAT64 route.</td></tr></table>	Option	Description	<i>disable</i>	Disable adding NAT64 route.	<i>enable</i>	Enable adding NAT64 route.			
Option	Description									
<i>disable</i>	Disable adding NAT64 route.									
<i>enable</i>	Enable adding NAT64 route.									

Parameter	Description	Type	Size	Default
client-cert	Enable/disable requesting client certificate.	option	-	enable
	Option Description			
	<i>disable</i>	Disable client certificate request.		
	<i>enable</i>	Enable client certificate request.		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	
comment	Comment.	var-string	Maximum length: 255	
embedded-ipv4-address	Enable/disable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.	option	-	disable
	Option Description			
	<i>disable</i>	Disable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.		
	<i>enable</i>	Enable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.		
empty-cert-action	Action for an empty client certificate.	option	-	block
	Option Description			
	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.		
	<i>block</i>	Block the SSL handshake if the client certificate is empty.		
	<i>accept-unmanageable</i>	Accept the SSL handshake only if the end-point is unmanageable.		
extip	IPv6 address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified	
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified	
h2-support	Enable/disable HTTP2 support (default = enable).	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable HTTP2 support.		
	<i>disable</i>	Disable HTTP2 support.		
h3-support	Enable/disable HTTP3/QUIC support (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HTTP3/QUIC support.		
	<i>disable</i>	Disable HTTP3/QUIC support.		
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).		
	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.		
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35	
http-cookie-share	Control sharing of cookies across virtual servers. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	Option	Description		
	<i>disable</i>	Only allow HTTP cookie to match this virtual server.		
	<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.		

Parameter	Description	Type	Size	Default						
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the X-Forwarded-For HTTP header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adding HTTP header.</td></tr><tr><td><i>disable</i></td><td>Disable adding HTTP header.</td></tr></table>	Option	Description	<i>enable</i>	Enable adding HTTP header.	<i>disable</i>	Disable adding HTTP header.			
Option	Description									
<i>enable</i>	Enable adding HTTP header.									
<i>disable</i>	Disable adding HTTP header.									
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35							
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP session multiplexing.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP session multiplexing.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP session multiplexing.	<i>disable</i>	Disable HTTP session multiplexing.			
Option	Description									
<i>enable</i>	Enable HTTP session multiplexing.									
<i>disable</i>	Disable HTTP session multiplexing.									
http-redirect	Enable/disable redirection of HTTP to HTTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redirection of HTTP to HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable redirection of HTTP to HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable redirection of HTTP to HTTPS.	<i>disable</i>	Disable redirection of HTTP to HTTPS.			
Option	Description									
<i>enable</i>	Enable redirection of HTTP to HTTPS.									
<i>disable</i>	Disable redirection of HTTP to HTTPS.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td><i>enable</i></td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>	Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.			
Option	Description									
<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.									
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.									
id	Custom defined ID.	integer	Minimum value: 0 0 Maximum value: 65535							
ipv4-mappedip	Range of mapped IP addresses. Specify the start IP address followed by a space and the end IP address.	user	Not Specified							

Parameter	Description	Type	Size	Default
ipv4-mappedport	IPv4 port number range on the destination network to which the external port number range is mapped.	user	Not Specified	
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option	Description		
	<i>static</i>	Distribute sessions based on source IP.		
	<i>round-robin</i>	Distribute sessions based round robin order.		
	<i>weighted</i>	Distribute sessions based on weight.		
	<i>least-session</i>	Sends new sessions to the server with the lowest session count.		
	<i>least-rtt</i>	Distribute new sessions to the server with lowest Round-Trip-Time.		
	<i>first-alive</i>	Distribute sessions to the first server that is alive.		
	<i>http-host</i>	Distribute sessions to servers based on host field in HTTP header.		
mappedip	Mapped IPv6 address range in the format startIP-endIP.	user	Not Specified	
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified	
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 1000 0 Maximum value: 100000	
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79	
name	Virtual ip6 name.	string	Maximum length: 79	
nat-source-vip	Enable to perform SNAT on traffic from mappedip to the extip for all egress interfaces.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable nat-source-vip.		
	<i>enable</i>	Perform SNAT on traffic from mappedip to the extip for all egress interfaces.		
nat64	Enable/disable DNAT64.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable DNAT64.		
	<i>enable</i>	Enable DNAT64.		
nat66	Enable/disable DNAT66.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable DNAT66.		
	<i>enable</i>	Enable DNAT66.		
ndp-reply	Enable/disable this FortiGate unit's ability to respond to NDP requests for this virtual IP address (default = enable).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this FortiGate unit's ability to respond to NDP requests for this virtual IP address.		
	<i>enable</i>	Enable this FortiGate unit's ability to respond to NDP requests for this virtual IP address.		
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Outlook Web Access support.		
	<i>enable</i>	Enable Outlook Web Access support.		
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>http-cookie</i>	HTTP cookie.		
	<i>ssl-session-id</i>	SSL session ID.		
portforward	Enable port forwarding.	option	-	disable

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable port forward.</td></tr><tr><td><i>enable</i></td><td>Enable/disable port forwarding.</td></tr></table>	Option	Description	<i>disable</i>	Disable port forward.	<i>enable</i>	Enable/disable port forwarding.																	
	Option	Description																						
	<i>disable</i>	Disable port forward.																						
<i>enable</i>	Enable/disable port forwarding.																							
protocol	Protocol to use when forwarding packets.	option	-	tcp																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>sctp</i></td><td>SCTP.</td></tr></table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>sctp</i>	SCTP.															
	Option	Description																						
	<i>tcp</i>	TCP.																						
	<i>udp</i>	UDP.																						
<i>sctp</i>	SCTP.																							
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>ssl</i></td><td>SSL.</td></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>ip</i></td><td>IP.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.	<i>imaps</i>	IMAPS.	<i>pop3s</i>	POP3S.	<i>smtps</i>	SMTPS.	<i>ssl</i>	SSL.	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>ip</i>	IP.			
	Option	Description																						
	<i>http</i>	HTTP.																						
	<i>https</i>	HTTPS.																						
	<i>imaps</i>	IMAPS.																						
	<i>pop3s</i>	POP3S.																						
	<i>smtps</i>	SMTPS.																						
	<i>ssl</i>	SSL.																						
	<i>tcp</i>	TCP.																						
	<i>udp</i>	UDP.																						
<i>ip</i>	IP.																							
src-filter <range>	Source IP6 filter (x:x:x:x:x:x/x). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79																					
src-vip-filter	Enable/disable use of 'src-filter' to match destinations for the reverse SNAT rule.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Match any destination for the reverse SNAT rule.</td></tr><tr><td><i>enable</i></td><td>Match only destinations in 'src-filter' for the reverse SNAT rule.</td></tr></table>	Option	Description	<i>disable</i>	Match any destination for the reverse SNAT rule.	<i>enable</i>	Match only destinations in 'src-filter' for the reverse SNAT rule.																	
	Option	Description																						
	<i>disable</i>	Match any destination for the reverse SNAT rule.																						
<i>enable</i>	Match only destinations in 'src-filter' for the reverse SNAT rule.																							

Parameter	Description	Type	Size	Default										
ssl-accept-ffdhe-groups	Enable/disable FFDHE cipher suite for SSL key exchange.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Accept FFDHE groups.</td></tr><tr><td><i>disable</i></td><td>Do not accept FFDHE groups.</td></tr></table>	Option	Description	<i>enable</i>	Accept FFDHE groups.	<i>disable</i>	Do not accept FFDHE groups.							
Option	Description													
<i>enable</i>	Accept FFDHE groups.													
<i>disable</i>	Do not accept FFDHE groups.													
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-	high										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>Use AES.</td></tr><tr><td><i>medium</i></td><td>Use AES, 3DES, or RC4.</td></tr><tr><td><i>low</i></td><td>Use AES, 3DES, RC4, or DES.</td></tr><tr><td><i>custom</i></td><td>Use config ssl-cipher-suites to select the cipher suites that are allowed.</td></tr></table>	Option	Description	<i>high</i>	Use AES.	<i>medium</i>	Use AES, 3DES, or RC4.	<i>low</i>	Use AES, 3DES, RC4, or DES.	<i>custom</i>	Use config ssl-cipher-suites to select the cipher suites that are allowed.			
Option	Description													
<i>high</i>	Use AES.													
<i>medium</i>	Use AES, 3DES, or RC4.													
<i>low</i>	Use AES, 3DES, RC4, or DES.													
<i>custom</i>	Use config ssl-cipher-suites to select the cipher suites that are allowed.													
ssl-certificate<name>	Name of the certificate to use for SSL handshake. Certificate list.	string	Maximum length: 79											
ssl-client-fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>enable</i></td><td>Enable.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.							
Option	Description													
<i>disable</i>	Disable.													
<i>enable</i>	Enable.													
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 0 200 Maximum value: 1048576											
ssl-client-renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-	secure										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow a SSL client to renegotiate.</td></tr><tr><td><i>deny</i></td><td>Abort any SSL connection that attempts to renegotiate.</td></tr></table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.							
Option	Description													
<i>allow</i>	Allow a SSL client to renegotiate.													
<i>deny</i>	Abort any SSL connection that attempts to renegotiate.													

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>secure</i></td><td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td></tr></table>		Option	Description	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.												
	Option	Description																
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.																	
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1000 1 Maximum value: 10000															
ssl-client-session-state-timeout	Number of minutes to keep client to FortiGate SSL session state.	integer	Minimum value: 30 1 Maximum value: 14400															
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-	both														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not keep session states.</td></tr><tr><td><i>time</i></td><td>Expire session states after this many minutes.</td></tr><tr><td><i>count</i></td><td>Expire session states when this maximum is reached.</td></tr><tr><td><i>both</i></td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>		Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.						
	Option	Description																
	<i>disable</i>	Do not keep session states.																
	<i>time</i>	Expire session states after this many minutes.																
	<i>count</i>	Expire session states when this maximum is reached.																
<i>both</i>	Expire session states based on time or count, whichever occurs first.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td><i>3072</i></td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td><i>4096</i></td><td>4096-bit Diffie-Hellman prime.</td></tr></table>		Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.		
	Option	Description																
	<i>768</i>	768-bit Diffie-Hellman prime.																
	<i>1024</i>	1024-bit Diffie-Hellman prime.																
	<i>1536</i>	1536-bit Diffie-Hellman prime.																
	<i>2048</i>	2048-bit Diffie-Hellman prime.																
	<i>3072</i>	3072-bit Diffie-Hellman prime.																
<i>4096</i>	4096-bit Diffie-Hellman prime.																	
ssl-hpkp	Enable/disable including HPKP header in response.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add a HPKP header to each HTTP response.</td></tr><tr><td><i>enable</i></td><td>Add a HPKP header to each a HTTP response.</td></tr></table>		Option	Description	<i>disable</i>	Do not add a HPKP header to each HTTP response.	<i>enable</i>	Add a HPKP header to each a HTTP response.										
	Option	Description																
	<i>disable</i>	Do not add a HPKP header to each HTTP response.																
<i>enable</i>	Add a HPKP header to each a HTTP response.																	

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>report-only</i></td><td>Add a HPKP Report-Only header to each HTTP response.</td></tr></table>	Option	Description	<i>report-only</i>	Add a HPKP Report-Only header to each HTTP response.					
Option	Description									
<i>report-only</i>	Add a HPKP Report-Only header to each HTTP response.									
ssl-hpkp-age	Number of minutes the web browser should keep HPKP.	integer	Minimum value: 60 Maximum value: 157680000	5184000						
ssl-hpkp-backup	Certificate to generate backup HPKP pin from.	string	Maximum length: 79							
ssl-hpkp-include-subdomains	Indicate that HPKP header applies to all subdomains.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>HPKP header does not apply to subdomains.</td></tr><tr><td><i>enable</i></td><td>HPKP header applies to subdomains.</td></tr></table>	Option	Description	<i>disable</i>	HPKP header does not apply to subdomains.	<i>enable</i>	HPKP header applies to subdomains.			
Option	Description									
<i>disable</i>	HPKP header does not apply to subdomains.									
<i>enable</i>	HPKP header applies to subdomains.									
ssl-hpkp-primary	Certificate to generate primary HPKP pin from.	string	Maximum length: 79							
ssl-hpkp-report-uri	URL to report HPKP violations to.	var-string	Maximum length: 255							
ssl-hsts	Enable/disable including HSTS header in response.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add a HSTS header to each a HTTP response.</td></tr><tr><td><i>enable</i></td><td>Add a HSTS header to each HTTP response.</td></tr></table>	Option	Description	<i>disable</i>	Do not add a HSTS header to each a HTTP response.	<i>enable</i>	Add a HSTS header to each HTTP response.			
Option	Description									
<i>disable</i>	Do not add a HSTS header to each a HTTP response.									
<i>enable</i>	Add a HSTS header to each HTTP response.									
ssl-hsts-age	Number of seconds the client should honor the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000						
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>HSTS header does not apply to subdomains.</td></tr><tr><td><i>enable</i></td><td>HSTS header applies to subdomains.</td></tr></table>	Option	Description	<i>disable</i>	HSTS header does not apply to subdomains.	<i>enable</i>	HSTS header applies to subdomains.			
Option	Description									
<i>disable</i>	HSTS header does not apply to subdomains.									
<i>enable</i>	HSTS header applies to subdomains.									

Parameter	Description	Type	Size	Default												
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP location conversion.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP location conversion.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP location conversion.	<i>disable</i>	Disable HTTP location conversion.									
Option	Description															
<i>enable</i>	Enable HTTP location conversion.															
<i>disable</i>	Disable HTTP location conversion.															
ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Match HTTP host in response header.</td></tr><tr><td><i>disable</i></td><td>Do not match HTTP host.</td></tr></table>	Option	Description	<i>enable</i>	Match HTTP host in response header.	<i>disable</i>	Do not match HTTP host.									
Option	Description															
<i>enable</i>	Match HTTP host in response header.															
<i>disable</i>	Do not match HTTP host.															
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.3												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-	tls-1.1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															
ssl-mode	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-	half												

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>half</i></td><td>Client to FortiGate SSL.</td></tr><tr><td><i>full</i></td><td>Client to FortiGate and FortiGate to Server SSL.</td></tr></table>	Option	Description	<i>half</i>	Client to FortiGate SSL.	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.									
	Option	Description														
	<i>half</i>	Client to FortiGate SSL.														
<i>full</i>	Client to FortiGate and FortiGate to Server SSL.															
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-	require												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>require</i></td><td>Allow only Diffie-Hellman cipher-suites, so PFS is applied.</td></tr><tr><td><i>deny</i></td><td>Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</td></tr><tr><td><i>allow</i></td><td>Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</td></tr></table>	Option	Description	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.	<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.							
	Option	Description														
	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.														
	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.														
<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.															
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send empty fragments.</td></tr><tr><td><i>disable</i></td><td>Do not send empty fragments.</td></tr></table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.									
	Option	Description														
	<i>enable</i>	Send empty fragments.														
<i>disable</i>	Do not send empty fragments.															
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	client												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>Use AES.</td></tr><tr><td><i>medium</i></td><td>Use AES, 3DES, or RC4.</td></tr><tr><td><i>low</i></td><td>Use AES, 3DES, RC4, or DES.</td></tr><tr><td><i>custom</i></td><td>Use config ssl-server-cipher-suites to select the cipher suites that are allowed.</td></tr><tr><td><i>client</i></td><td>Use the same encryption algorithms for client and server sessions.</td></tr></table>	Option	Description	<i>high</i>	Use AES.	<i>medium</i>	Use AES, 3DES, or RC4.	<i>low</i>	Use AES, 3DES, RC4, or DES.	<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.	<i>client</i>	Use the same encryption algorithms for client and server sessions.			
	Option	Description														
	<i>high</i>	Use AES.														
	<i>medium</i>	Use AES, 3DES, or RC4.														
	<i>low</i>	Use AES, 3DES, RC4, or DES.														
	<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.														
<i>client</i>	Use the same encryption algorithms for client and server sessions.															

Parameter	Description	Type	Size	Default														
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr><tr><td>client</td><td>Use same value as client configuration.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.	client	Use same value as client configuration.			
Option	Description																	
ssl-3.0	SSL 3.0.																	
tls-1.0	TLS 1.0.																	
tls-1.1	TLS 1.1.																	
tls-1.2	TLS 1.2.																	
tls-1.3	TLS 1.3.																	
client	Use same value as client configuration.																	
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr><tr><td>client</td><td>Use same value as client configuration.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.	client	Use same value as client configuration.			
Option	Description																	
ssl-3.0	SSL 3.0.																	
tls-1.0	TLS 1.0.																	
tls-1.1	TLS 1.1.																	
tls-1.2	TLS 1.2.																	
tls-1.3	TLS 1.3.																	
client	Use same value as client configuration.																	
ssl-server-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable secure renegotiation.</td></tr><tr><td>disable</td><td>Disable secure renegotiation.</td></tr></table>	Option	Description	enable	Enable secure renegotiation.	disable	Disable secure renegotiation.											
Option	Description																	
enable	Enable secure renegotiation.																	
disable	Disable secure renegotiation.																	
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 100 1 Maximum value: 10000															
ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 60 1 Maximum value: 14400															

Parameter	Description	Type	Size	Default										
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not keep session states.</td></tr><tr><td>time</td><td>Expire session states after this many minutes.</td></tr><tr><td>count</td><td>Expire session states when this maximum is reached.</td></tr><tr><td>both</td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>	Option	Description	disable	Do not keep session states.	time	Expire session states after this many minutes.	count	Expire session states when this maximum is reached.	both	Expire session states based on time or count, whichever occurs first.			
Option	Description													
disable	Do not keep session states.													
time	Expire session states after this many minutes.													
count	Expire session states when this maximum is reached.													
both	Expire session states based on time or count, whichever occurs first.													
type	Configure a static NAT server load balance VIP or access proxy.	option	-	static-nat										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static-nat</td><td>Static NAT.</td></tr><tr><td>server-load-balance</td><td>Server load balance.</td></tr><tr><td>access-proxy</td><td>Access proxy.</td></tr></table>	Option	Description	static-nat	Static NAT.	server-load-balance	Server load balance.	access-proxy	Access proxy.					
Option	Description													
static-nat	Static NAT.													
server-load-balance	Server load balance.													
access-proxy	Access proxy.													
user-agent-detect	Enable/disable detecting device type by HTTP user-agent if no client certificate is provided.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable detecting unknown devices by HTTP user-agent if no client certificate is provided.</td></tr><tr><td>enable</td><td>Enable detecting unknown devices by HTTP user-agent if no client certificate is provided.</td></tr></table>	Option	Description	disable	Disable detecting unknown devices by HTTP user-agent if no client certificate is provided.	enable	Enable detecting unknown devices by HTTP user-agent if no client certificate is provided.							
Option	Description													
disable	Disable detecting unknown devices by HTTP user-agent if no client certificate is provided.													
enable	Enable detecting unknown devices by HTTP user-agent if no client certificate is provided.													
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000										
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add HTTP header indicating SSL offload for WebLogic server.</td></tr><tr><td>enable</td><td>Add HTTP header indicating SSL offload for WebLogic server.</td></tr></table>	Option	Description	disable	Do not add HTTP header indicating SSL offload for WebLogic server.	enable	Add HTTP header indicating SSL offload for WebLogic server.							
Option	Description													
disable	Do not add HTTP header indicating SSL offload for WebLogic server.													
enable	Add HTTP header indicating SSL offload for WebLogic server.													

Parameter	Description	Type	Size	Default
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable
Option	Description			
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.			
<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.			

config quic

Parameter	Description	Type	Size	Default
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2
active-migration	Enable/disable active migration (default = disable).	option	-	disable
Option	Description			
<i>enable</i>	Enable active migration.			
<i>disable</i>	Disable active migration.			
grease-quic-bit	Enable/disable grease QUIC bit (default = enable).	option	-	enable
Option	Description			
<i>enable</i>	Enable grease QUIC bit.			
<i>disable</i>	Disable grease QUIC bit.			
max-ack-delay	Maximum ACK delay in milliseconds (1 - 16383, default = 25).	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes (1 - 1500, default = 1500).	integer	Minimum value: 1 Maximum value: 1500	1500

Parameter	Description	Type	Size	Default
max-idle-timeout	Maximum idle timeout milliseconds (1 - 60000, default = 30000).	integer	Minimum value: 1 Maximum value: 60000	30000
max-udp-payload-size	Maximum UDP payload size in bytes (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500

config realservers

Parameter	Description	Type	Size	Default								
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified									
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	vip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable per server health check.</td></tr><tr><td>enable</td><td>Enable per server health check.</td></tr><tr><td>vip</td><td>Use health check defined in VIP.</td></tr></table>	Option	Description	disable	Disable per server health check.	enable	Enable per server health check.	vip	Use health check defined in VIP.			
Option	Description											
disable	Disable per server health check.											
enable	Enable per server health check.											
vip	Use health check defined in VIP.											
holddown-interval	Time in seconds that the system waits before re-activating a previously down active server in the active-standby mode. This is to prevent any flapping issues.	integer	Minimum value: 30 Maximum value: 65535	300								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
ip	IP address of the real server.	user	Not Specified									
max-connections	Max number of active connections that can be directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0								
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default								
	Health monitor name.											
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 0 1 Maximum value: 65535									
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>active</td><td>Server status active.</td></tr><tr><td>standby</td><td>Server status standby.</td></tr><tr><td>disable</td><td>Server status disable.</td></tr></table>	Option	Description	active	Server status active.	standby	Server status standby.	disable	Server status disable.			
Option	Description											
active	Server status active.											
standby	Server status standby.											
disable	Server status disable.											
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable virtual hostname/IP translation.</td></tr><tr><td>disable</td><td>Disable virtual hostname/IP translation.</td></tr></table>	Option	Description	enable	Enable virtual hostname/IP translation.	disable	Disable virtual hostname/IP translation.					
Option	Description											
enable	Enable virtual hostname/IP translation.											
disable	Disable virtual hostname/IP translation.											
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 1 Maximum value: 255									

config ssl-cipher-suites

Parameter	Description	Type	Size	Default								
cipher	Cipher suite name.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr></table>	Option	Description	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.			
Option	Description											
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.											
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.											
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-RSA-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-AES-256-GCM-SHA384</td><td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr></table>	Option	Description	TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.			
Option	Description																									
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																									
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																									
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																									
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.																									
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.																									
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.																									
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.																									
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.																									
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.																									
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																									

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																						
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																						
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																						
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																						
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																						
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																						
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																						
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																						
<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																							
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																							
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295	0																				
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3																				

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config ssl-server-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	
	Option	Description		
	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.		
	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.		
	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.</td></tr></table>	Option	Description	TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.	TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.			
Option	Description																											
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																											
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																											
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																											
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																											
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																											
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																											
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																											
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																											
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																											
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.																											
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		
TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.		
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																		
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																			
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295																	
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																		
	<i>ssl-3.0</i>	SSL 3.0.																		
	<i>tls-1.0</i>	TLS 1.0.																		
	<i>tls-1.1</i>	TLS 1.1.																		
	<i>tls-1.2</i>	TLS 1.2.																		
<i>tls-1.3</i>	TLS 1.3.																			

config firewall vipgrp

Configure IPv4 virtual IP groups.

```
config firewall vipgrp
  Description: Configure IPv4 virtual IP groups.
  edit <name>
    set color {integer}
    set comments {var-string}
    set interface {string}
    set member <name1>, <name2>, ...
    set uuid {uuid}
  next
end
```

config firewall vipgrp

Parameter	Description	Type	Size	Default
color	Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
interface	Interface.	string	Maximum length: 35	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP name.	string	Maximum length: 79	
name	VIP group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config firewall vipgrp6

Configure IPv6 virtual IP groups.

```
config firewall vipgrp6
  Description: Configure IPv6 virtual IP groups.
  edit <name>
```

```

        set color {integer}
        set comments {var-string}
        set member <name1>, <name2>, ...
        set uuid {uuid}
    next
end

```

config firewall vipgrp6

Parameter	Description	Type	Size	Default
color	Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). IPv6 VIP name.	string	Maximum length: 79	
name	IPv6 VIP group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config firewall wildcard-fqdn custom

Config global/VDOM Wildcard FQDN address.

```

config firewall wildcard-fqdn custom
    Description: Config global/VDOM Wildcard FQDN address.
    edit <name>
        set color {integer}
        set comment {var-string}
        set uuid {uuid}
        set wildcard-fqdn {string}
    next
end

```

config firewall wildcard-fqdn custom

Parameter	Description	Type	Size	Default
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
name	Address name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255	

config firewall wildcard-fqdn group

Config global Wildcard FQDN address groups.

```
config firewall wildcard-fqdn group
  Description: Config global Wildcard FQDN address groups.
  edit <name>
    set color {integer}
    set comment {var-string}
    set member <name1>, <name2>, ...
    set uuid {uuid}
  next
end
```

config firewall wildcard-fqdn group

Parameter	Description	Type	Size	Default
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
member <name>	Address group members. Address name.	string	Maximum length: 79	
name	Address group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000- 0000-0000- 000000000000

ftp-proxy

This section includes syntax for the following commands:

- [config ftp-proxy explicit on page 733](#)

config ftp-proxy explicit

Configure explicit FTP proxy settings.

```
config ftp-proxy explicit
    Description: Configure explicit FTP proxy settings.
    set incoming-ip {ipv4-address-any}
    set incoming-port {user}
    set outgoing-ip {ipv4-address-any}
    set sec-default-action [accept|deny]
    set server-data-mode [client|passive]
    set ssl [enable|disable]
    set ssl-algorithm [high|medium|...]
    set ssl-cert <name1>, <name2>, ...
    set ssl-dh-bits [768|1024|...]
    set status [enable|disable]
end
```

config ftp-proxy explicit

Parameter	Description	Type	Size	Default
incoming-ip	Accept incoming FTP requests from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0
incoming-port	Accept incoming FTP requests on one or more ports.	user	Not Specified	
outgoing-ip	Outgoing FTP requests will leave from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	
sec-default-action	Accept or deny explicit FTP proxy sessions when no FTP proxy firewall policy exists.	option	-	deny

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not</td></tr><tr><td><i>deny</i></td><td>Deny requests unless there is a matching explicit FTP proxy policy.</td></tr></table>	Option	Description	<i>accept</i>	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not	<i>deny</i>	Deny requests unless there is a matching explicit FTP proxy policy.							
	Option	Description												
	<i>accept</i>	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not												
<i>deny</i>	Deny requests unless there is a matching explicit FTP proxy policy.													
server-data-mode	Determine mode of data session on FTP server side.	option	-	client										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>client</i></td><td>Use the same transmission mode for client and server data sessions.</td></tr><tr><td><i>passive</i></td><td>Use passive mode on server data session.</td></tr></table>	Option	Description	<i>client</i>	Use the same transmission mode for client and server data sessions.	<i>passive</i>	Use passive mode on server data session.							
	Option	Description												
	<i>client</i>	Use the same transmission mode for client and server data sessions.												
<i>passive</i>	Use passive mode on server data session.													
ssl	Enable/disable the explicit FTPS proxy.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the explicit FTPS proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the explicit FTPS proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable the explicit FTPS proxy.	<i>disable</i>	Disable the explicit FTPS proxy.							
	Option	Description												
	<i>enable</i>	Enable the explicit FTPS proxy.												
<i>disable</i>	Disable the explicit FTPS proxy.													
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.					
	Option	Description												
	<i>high</i>	High encryption. Allow only AES and ChaCha												
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.												
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.													
ssl-cert <name>	List of certificate names to use for SSL connections to this server. Certificate list.	string	Maximum length: 79											
ssl-dh-bits	Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).	option	-	2048										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.			
	Option	Description												
	<i>768</i>	768-bit Diffie-Hellman prime.												
	<i>1024</i>	1024-bit Diffie-Hellman prime.												
	<i>1536</i>	1536-bit Diffie-Hellman prime.												
<i>2048</i>	2048-bit Diffie-Hellman prime.													
status	Enable/disable the explicit FTP proxy.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the explicit FTP proxy.		
	<i>disable</i>	Disable the explicit FTP proxy.		

icap

This section includes syntax for the following commands:

- [config icap profile on page 736](#)
- [config icap server-group on page 744](#)
- [config icap server on page 743](#)

config icap profile

Configure ICAP profiles.

```
config icap profile
  Description: Configure ICAP profiles.
  edit <name>
    set 204-response [disable|enable]
    set 204-size-limit {integer}
    set chunk-encap [disable|enable]
    set comment {var-string}
    set extension-feature {option1}, {option2}, ...
    set file-transfer {option1}, {option2}, ...
    set file-transfer-failure [error|bypass]
    set file-transfer-path {string}
    set file-transfer-server {string}
    set icap-block-log [disable|enable]
  config icap-headers
    Description: Configure ICAP forwarded request headers.
    edit <id>
      set base64-encoding [disable|enable]
      set content {string}
      set name {string}
    next
  end
  set methods {option1}, {option2}, ...
  set ocr-only [disable|enable]
  set preview [disable|enable]
  set preview-data-length {integer}
  set replacemsg-group {string}
  set request [disable|enable]
  set request-failure [error|bypass]
  set request-path {string}
  set request-server {string}
  set respmod-default-action [forward|bypass]
  config respmod-forward-rules
    Description: ICAP response mode forward rules.
    edit <name>
```



```

        set action [forward|bypass]
        config header-group
            Description: HTTP header group.
            edit <id>
                set case-sensitivity [disable|enable]
                set header {string}
                set header-name {string}
            next
        end
        set host {string}
        set http-resp-status-code <code1>, <code2>, ...
    next
end
set response [disable|enable]
set response-failure [error|bypass]
set response-path {string}
set response-req-hdr [disable|enable]
set response-server {string}
set scan-progress-interval {integer}
set streaming-content-bypass [disable|enable]
set timeout {integer}
next
end

```

config icap profile

Parameter	Description	Type	Size	Default						
204-response	Enable/disable allowance of 204 response from ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable allowance of 204 response from ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable allowance of 204 response from ICAP server.</td></tr></table>	Option	Description	<i>disable</i>	Disable allowance of 204 response from ICAP server.	<i>enable</i>	Enable allowance of 204 response from ICAP server.			
Option	Description									
<i>disable</i>	Disable allowance of 204 response from ICAP server.									
<i>enable</i>	Enable allowance of 204 response from ICAP server.									
204-size-limit	204 response size limit to be saved by ICAP client in megabytes (1 - 10, default = 1 MB).	integer	Minimum value: 1 Maximum value: 10	1						
chunk-encap	Enable/disable chunked encapsulation (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not encapsulate chunked data.</td></tr><tr><td><i>enable</i></td><td>Encapsulate chunked data into a new chunk.</td></tr></table>	Option	Description	<i>disable</i>	Do not encapsulate chunked data.	<i>enable</i>	Encapsulate chunked data into a new chunk.			
Option	Description									
<i>disable</i>	Do not encapsulate chunked data.									
<i>enable</i>	Encapsulate chunked data into a new chunk.									

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
extension-feature	Enable/disable ICAP extension features.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>scan-progress</td><td>Support X-Scan-Progress-Interval ICAP header.</td></tr></table>	Option	Description	scan-progress	Support X-Scan-Progress-Interval ICAP header.					
Option	Description									
scan-progress	Support X-Scan-Progress-Interval ICAP header.									
file-transfer	Configure the file transfer protocols to pass transferred files to an ICAP server as REQMOD.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssh</td><td>Forward file transfer with SSH protocol to ICAP server for further processing.</td></tr><tr><td>ftp</td><td>Forward file transfer with FTP protocol to ICAP server for further processing.</td></tr></table>	Option	Description	ssh	Forward file transfer with SSH protocol to ICAP server for further processing.	ftp	Forward file transfer with FTP protocol to ICAP server for further processing.			
Option	Description									
ssh	Forward file transfer with SSH protocol to ICAP server for further processing.									
ftp	Forward file transfer with FTP protocol to ICAP server for further processing.									
file-transfer-failure	Action to take if the ICAP server cannot be contacted when processing a file transfer.	option	-	error						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>error</td><td>Error.</td></tr><tr><td>bypass</td><td>Bypass.</td></tr></table>	Option	Description	error	Error.	bypass	Bypass.			
Option	Description									
error	Error.									
bypass	Bypass.									
file-transfer-path	Path component of the ICAP URI that identifies the file transfer processing service.	string	Maximum length: 127							
file-transfer-server	ICAP server to use for a file transfer.	string	Maximum length: 63							
icap-block-log	Enable/disable UTM log when infection found (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable UTM log when infection found.</td></tr><tr><td>enable</td><td>Enable UTM log when infection found.</td></tr></table>	Option	Description	disable	Disable UTM log when infection found.	enable	Enable UTM log when infection found.			
Option	Description									
disable	Disable UTM log when infection found.									
enable	Enable UTM log when infection found.									
methods	The allowed HTTP methods that will be sent to ICAP server for further processing.	option	-	delete get head options post put trace connect other						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>delete</i>	Forward HTTP request or response with DELETE method to ICAP server for further processing.		
	<i>get</i>	Forward HTTP request or response with GET method to ICAP server for further processing.		
	<i>head</i>	Forward HTTP request or response with HEAD method to ICAP server for further processing.		
	<i>options</i>	Forward HTTP request or response with OPTIONS method to ICAP server for further processing.		
	<i>post</i>	Forward HTTP request or response with POST method to ICAP server for further processing.		
	<i>put</i>	Forward HTTP request or response with PUT method to ICAP server for further processing.		
	<i>trace</i>	Forward HTTP request or response with TRACE method to ICAP server for further processing.		
	<i>connect</i>	Forward HTTP request or response with CONNECT method to ICAP server for further processing.		
	<i>other</i>	Forward HTTP request or response with All other methods to ICAP server for further processing.		
name	ICAP profile name.	string	Maximum length: 47	
ocr-only	Enable/disable this FortiGate unit to submit only OCR interested content to the ICAP server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable this FortiGate unit to submit only OCR interested content to the ICAP server.		
	<i>enable</i>	Enable this FortiGate unit to submit only OCR interested content to the ICAP server.		
preview	Enable/disable preview of data to ICAP server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable preview of data to ICAP server.		
	<i>enable</i>	Enable preview of data to ICAP server.		

Parameter	Description	Type	Size	Default						
preview-data-length	Preview data length to be sent to ICAP server.	integer	Minimum value: 0 Maximum value: 4096	0						
replacemsg-group	Replacement message group.	string	Maximum length: 35							
request	Enable/disable whether an HTTP request is passed to an ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable HTTP request passing to ICAP server.</td></tr><tr><td>enable</td><td>Enable HTTP request passing to ICAP server.</td></tr></table>	Option	Description	disable	Disable HTTP request passing to ICAP server.	enable	Enable HTTP request passing to ICAP server.			
Option	Description									
disable	Disable HTTP request passing to ICAP server.									
enable	Enable HTTP request passing to ICAP server.									
request-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP request.	option	-	error						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>error</td><td>Error.</td></tr><tr><td>bypass</td><td>Bypass.</td></tr></table>	Option	Description	error	Error.	bypass	Bypass.			
Option	Description									
error	Error.									
bypass	Bypass.									
request-path	Path component of the ICAP URI that identifies the HTTP request processing service.	string	Maximum length: 127							
request-server	ICAP server to use for an HTTP request.	string	Maximum length: 63							
respmod-default-action	Default action to ICAP response modification (respmod) processing.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>forward</td><td>Forward response to ICAP server unless a rule specifies not to.</td></tr><tr><td>bypass</td><td>Don't forward request to ICAP server unless a rule specifies to forward the request.</td></tr></table>	Option	Description	forward	Forward response to ICAP server unless a rule specifies not to.	bypass	Don't forward request to ICAP server unless a rule specifies to forward the request.			
Option	Description									
forward	Forward response to ICAP server unless a rule specifies not to.									
bypass	Don't forward request to ICAP server unless a rule specifies to forward the request.									
response	Enable/disable whether an HTTP response is passed to an ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable HTTP response passing to ICAP server.</td></tr><tr><td>enable</td><td>Enable HTTP response passing to ICAP server.</td></tr></table>	Option	Description	disable	Disable HTTP response passing to ICAP server.	enable	Enable HTTP response passing to ICAP server.			
Option	Description									
disable	Disable HTTP response passing to ICAP server.									
enable	Enable HTTP response passing to ICAP server.									
response-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP response.	option	-	error						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error</i></td><td>Error.</td></tr><tr><td><i>bypass</i></td><td>Bypass.</td></tr></table>	Option	Description	<i>error</i>	Error.	<i>bypass</i>	Bypass.			
	Option	Description								
	<i>error</i>	Error.								
<i>bypass</i>	Bypass.									
response-path	Path component of the ICAP URI that identifies the HTTP response processing service.	string	Maximum length: 127							
response-req-hdr	Enable/disable addition of req-hdr for ICAP response modification (respmod) processing.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add req-hdr for response modification (respmod) processing.</td></tr><tr><td><i>enable</i></td><td>Add req-hdr for response modification (respmod) processing.</td></tr></table>	Option	Description	<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.	<i>enable</i>	Add req-hdr for response modification (respmod) processing.			
	Option	Description								
	<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.								
<i>enable</i>	Add req-hdr for response modification (respmod) processing.									
response-server	ICAP server to use for an HTTP response.	string	Maximum length: 63							
scan-progress-interval	Scan progress interval value.	integer	Minimum value: 5 Maximum value: 30	10						
streaming-content-bypass	Enable/disable bypassing of ICAP server for streaming content.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable bypassing of ICAP server for streaming content.</td></tr><tr><td><i>enable</i></td><td>Enable bypassing of ICAP server for streaming content.</td></tr></table>	Option	Description	<i>disable</i>	Disable bypassing of ICAP server for streaming content.	<i>enable</i>	Enable bypassing of ICAP server for streaming content.			
	Option	Description								
	<i>disable</i>	Disable bypassing of ICAP server for streaming content.								
<i>enable</i>	Enable bypassing of ICAP server for streaming content.									
timeout	Time (in seconds) that ICAP client waits for the response from ICAP server.	integer	Minimum value: 30 Maximum value: 3600	30						

config icap-headers

Parameter	Description	Type	Size	Default				
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of base64 encoding of HTTP content.</td></tr></table>				Option	Description	<i>disable</i>	Disable use of base64 encoding of HTTP content.
Option	Description							
<i>disable</i>	Disable use of base64 encoding of HTTP content.							

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable use of base64 encoding of HTTP content.		
content	HTTP header content.	string	Maximum length: 255	
id	HTTP forwarded header ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	HTTP forwarded header name.	string	Maximum length: 79	

config respmod-forward-rules

Parameter	Description	Type	Size	Default
action	Action to be taken for ICAP server.	option	-	forward
	Option	Description		
	<i>forward</i>	Forward request to ICAP server when this rule is matched.		
	<i>bypass</i>	Don't forward request to ICAP server when this rule is matched.		
host	Address object for the host.	string	Maximum length: 79	
http-resp-status-code <code>	HTTP response status code. HTTP response status code.	integer	Minimum value: 100 Maximum value: 599	
name	Address name.	string	Maximum length: 63	

config header-group

Parameter	Description	Type	Size	Default						
case-sensitivity	Enable/disable case sensitivity when matching header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Ignore case when matching header.</td></tr><tr><td><i>enable</i></td><td>Do not ignore case when matching header.</td></tr></table>				Option	Description	<i>disable</i>	Ignore case when matching header.	<i>enable</i>	Do not ignore case when matching header.
Option	Description									
<i>disable</i>	Ignore case when matching header.									
<i>enable</i>	Do not ignore case when matching header.									

Parameter	Description	Type	Size	Default
header	HTTP header regular expression.	string	Maximum length: 255	
header-name	HTTP header.	string	Maximum length: 79	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config icap server

Configure ICAP servers.

```

config icap server
  Description: Configure ICAP servers.
  edit <name>
    set addr-type [ip4|ip6|...]
    set fqdn {string}
    set healthcheck [disable|enable]
    set healthcheck-service {string}
    set ip-address {ipv4-address-any}
    set ip6-address {ipv6-address}
    set max-connections {integer}
    set port {integer}
    set secure [disable|enable]
    set ssl-cert {string}
  next
end

```

config icap server

Parameter	Description	Type	Size	Default								
addr-type	Address type of the remote ICAP server: IPv4, IPv6 or FQDN.	option	-	ip4								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip4</i></td><td>Use an IPv4 address for the remote ICAP server.</td></tr><tr><td><i>ip6</i></td><td>Use an IPv6 address for the remote ICAP server.</td></tr><tr><td><i>fqdn</i></td><td>Use the FQDN for the forwarding proxy server.</td></tr></table>	Option	Description	<i>ip4</i>	Use an IPv4 address for the remote ICAP server.	<i>ip6</i>	Use an IPv6 address for the remote ICAP server.	<i>fqdn</i>	Use the FQDN for the forwarding proxy server.			
Option	Description											
<i>ip4</i>	Use an IPv4 address for the remote ICAP server.											
<i>ip6</i>	Use an IPv6 address for the remote ICAP server.											
<i>fqdn</i>	Use the FQDN for the forwarding proxy server.											

Parameter	Description	Type	Size	Default						
fqdn	ICAP remote server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255							
healthcheck	Enable/disable ICAP remote server health checking. Attempts to connect to the remote ICAP server to verify that the server is operating normally.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable health checking.</td></tr><tr><td>enable</td><td>Enable health checking.</td></tr></table>				Option	Description	disable	Disable health checking.	enable	Enable health checking.
Option	Description									
disable	Disable health checking.									
enable	Enable health checking.									
healthcheck-service	ICAP Service name to use for health checks.	string	Maximum length: 127							
ip-address	IPv4 address of the ICAP server.	ipv4-address-any	Not Specified	0.0.0.0						
ip6-address	IPv6 address of the ICAP server.	ipv6-address	Not Specified	::						
max-connections	Maximum number of concurrent connections to ICAP server (unlimited = 0, default = 100). Must not be less than wad-worker-count.	integer	Minimum value: 0 Maximum value: 4294967295	100						
name	Server name.	string	Maximum length: 63							
port	ICAP server port.	integer	Minimum value: 1 Maximum value: 65535	1344						
secure	Enable/disable secure connection to ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable connection to secure ICAP server.</td></tr><tr><td>enable</td><td>Enable connection to secure ICAP server.</td></tr></table>				Option	Description	disable	Disable connection to secure ICAP server.	enable	Enable connection to secure ICAP server.
Option	Description									
disable	Disable connection to secure ICAP server.									
enable	Enable connection to secure ICAP server.									
ssl-cert	CA certificate name.	string	Maximum length: 79							

config icap server-group

Configure an ICAP server group consisting of multiple forward servers. Supports failover and load balancing.


```

config icap server-group
    Description: Configure an ICAP server group consisting of multiple forward servers. Supports
    failover and load balancing.
    edit <name>
        set ldb-method [weighted|least-session|...]
        config server-list
            Description: Add ICAP servers to a list to form a server group. Optionally assign
weights to each server.
            edit <name>
                set weight {integer}
            next
        end
    next
end

```

config icap server-group

Parameter	Description	Type	Size	Default								
ldb-method	Load balance method.	option	-	weighted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weighted</i></td><td>Load balance traffic to forward servers based on assigned weights.</td></tr><tr><td><i>least-session</i></td><td>Send new sessions to the server with lowest session count.</td></tr><tr><td><i>active-passive</i></td><td>Send new sessions to active server with high weight.</td></tr></table>	Option	Description	<i>weighted</i>	Load balance traffic to forward servers based on assigned weights.	<i>least-session</i>	Send new sessions to the server with lowest session count.	<i>active-passive</i>	Send new sessions to active server with high weight.			
Option	Description											
<i>weighted</i>	Load balance traffic to forward servers based on assigned weights.											
<i>least-session</i>	Send new sessions to the server with lowest session count.											
<i>active-passive</i>	Send new sessions to active server with high weight.											
name	Configure an ICAP server group consisting one or multiple forward servers. Supports failover and load balancing.	string	Maximum length: 63									

config server-list

Parameter	Description	Type	Size	Default
name	ICAP server name.	string	Maximum length: 63	
weight	Optionally assign a weight of the forwarding server for weighted load balancing (1 - 100, default = 10).	integer	Minimum value: 1 Maximum value: 100	10

ips

This section includes syntax for the following commands:

- [config ips custom on page 746](#)
- [config ips decoder on page 748](#)
- [config ips global on page 748](#)
- [config ips rule-settings on page 755](#)
- [config ips rule on page 753](#)
- [config ips sensor on page 755](#)
- [config ips settings on page 761](#)
- [config ips view-map on page 762](#)

config ips custom

Configure IPS custom signature.

```
config ips custom
  Description: Configure IPS custom signature.
  edit <tag>
    set action [pass|block]
    set application {user}
    set comment {string}
    set location {user}
    set log [disable|enable]
    set log-packet [disable|enable]
    set os {user}
    set protocol {user}
    set rule-id {integer}
    set severity {user}
    set signature {var-string}
    set status [disable|enable]
  next
end
```

config ips custom

Parameter	Description	Type	Size	Default
action	Default action (pass or block) for this signature.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
application	Applications to be protected. Blank for all applications.	user	Not Specified	
comment	Comment.	string	Maximum length: 63	
location	Protect client or server traffic.	user	Not Specified	
log	Enable/disable logging.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
log-packet	Enable/disable packet logging.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable packet logging.		
	<i>enable</i>	Enable packet logging.		
os	Operating system(s) that the signature protects. Blank for all operating systems.	user	Not Specified	
protocol	Protocol(s) that the signature scans. Blank for all protocols.	user	Not Specified	
rule-id	Signature ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	
signature	Custom signature enclosed in single quotes.	var-string	Maximum length: 4095	
status	Enable/disable this signature.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable status.		
tag	Signature tag.	string	Maximum length: 63	

config ips decoder

Configure IPS decoder. Read-only.

```

config ips decoder
  Description: Configure IPS decoder. Read-only.
  edit <name>
    config parameter
      Description: IPS group parameters. Read-only.
      edit <name>
        set value {string}
      next
    end
  next
end

```

config ips decoder

Parameter	Description	Type	Size	Default
name	Decoder name.	string	Maximum length: 63	

config parameter

Parameter	Description	Type	Size	Default
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

config ips global

Configure IPS global parameter.

```

config ips global
    Description: Configure IPS global parameter.
    set anomaly-mode [periodical|continuous]
    set av-mem-limit {integer}
    set cp-accel-mode [none|basic|...]
    set database [regular|extended]
    set deep-app-insp-db-limit {integer}
    set deep-app-insp-timeout {integer}
    set engine-count {integer}
    set exclude-signatures [none|ot]
    set fail-open [enable|disable]
    set ips-reserve-cpu [disable|enable]
    set machine-learning-detection [enable|disable]
    set ngfw-max-scan-range {integer}
    set np-accel-mode [none|basic]
    set packet-log-queue-depth {integer}
    set session-limit-mode [accurate|heuristic]
    set socket-size {integer}
    set sync-session-ttl [enable|disable]
    config tls-active-probe
        Description: TLS active probe configuration.
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set source-ip {ipv4-address}
        set source-ip6 {ipv6-address}
        set vdom {string}
    end
    set traffic-submit [enable|disable]
end

```

config ips global

Parameter	Description	Type	Size	Default						
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-	continuous						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>periodical</i></td><td>After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.</td></tr><tr><td><i>continuous</i></td><td>Block packets once an anomaly is detected. Overrides individual anomaly settings.</td></tr></table>				Option	Description	<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.	<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.
Option	Description									
<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.									
<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.									
av-mem-limit	Maximum percentage of system memory allowed for use on AV scanning (10 - 50, default = zero). To disable set to zero. When disabled, there is no limit on the AV memory usage.	integer	Minimum value: 0 10 Maximum value: 50							

Parameter	Description	Type	Size	Default								
cp-accel-mode *	IPS Pattern matching acceleration/offloading to CPx processors.	option	-	advanced **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>CPx acceleration/offloading disabled.</td></tr><tr><td>basic</td><td>Offload basic pattern matching to CPx processors.</td></tr><tr><td>advanced</td><td>Offload more types of pattern matching resulting in higher throughput than basic mode.</td></tr></table>	Option	Description	none	CPx acceleration/offloading disabled.	basic	Offload basic pattern matching to CPx processors.	advanced	Offload more types of pattern matching resulting in higher throughput than basic mode.			
Option	Description											
none	CPx acceleration/offloading disabled.											
basic	Offload basic pattern matching to CPx processors.											
advanced	Offload more types of pattern matching resulting in higher throughput than basic mode.											
database	Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.	option	-	extended **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>regular</td><td>IPS regular database package.</td></tr><tr><td>extended</td><td>IPS extended database package.</td></tr></table>	Option	Description	regular	IPS regular database package.	extended	IPS extended database package.					
Option	Description											
regular	IPS regular database package.											
extended	IPS extended database package.											
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database (1 - 2147483647, use recommended setting = 0).	integer	Minimum value: 0 0 Maximum value: 2147483647									
deep-app-insp-timeout	Timeout for Deep application inspection (1 - 2147483647 sec., 0 = use recommended setting).	integer	Minimum value: 0 0 Maximum value: 2147483647									
engine-count	Number of IPS engines running. If set to the default value of 0, FortiOS sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 0 Maximum value: 255									
exclude-signatures	Excluded signatures.	option	-	ot								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No signatures excluded.</td></tr><tr><td>ot</td><td>Exclude ot signatures.</td></tr></table>	Option	Description	none	No signatures excluded.	ot	Exclude ot signatures.					
Option	Description											
none	No signatures excluded.											
ot	Exclude ot signatures.											
fail-open	Enable to allow traffic if the IPS buffer is full. Default is disable and IPS traffic is blocked when the IPS buffer is full.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS fail open.</td></tr><tr><td><i>disable</i></td><td>Disable IPS fail open.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS fail open.	<i>disable</i>	Disable IPS fail open.			
	Option	Description								
	<i>enable</i>	Enable IPS fail open.								
<i>disable</i>	Disable IPS fail open.									
ips-reserve-cpu *	Enable/disable IPS daemon's use of CPUs other than CPU 0.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).</td></tr><tr><td><i>enable</i></td><td>Enable IPS daemon's use of CPUs other than CPU 0.</td></tr></table>	Option	Description	<i>disable</i>	Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).	<i>enable</i>	Enable IPS daemon's use of CPUs other than CPU 0.			
	Option	Description								
	<i>disable</i>	Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).								
<i>enable</i>	Enable IPS daemon's use of CPUs other than CPU 0.									
machine-learning-detection	Enable/disable machine learning detection.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ML detection.</td></tr><tr><td><i>disable</i></td><td>Disable ML detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable ML detection.	<i>disable</i>	Disable ML detection.			
	Option	Description								
	<i>enable</i>	Enable ML detection.								
<i>disable</i>	Disable ML detection.									
ngfw-max-scan-range	NGFW policy-mode app detection threshold.	integer	Minimum value: 4096 0 Maximum value: 4294967295							
np-accel-mode *	Acceleration mode for IPS processing by NPx processors.	option	-	basic						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>NPx acceleration disabled.</td></tr><tr><td><i>basic</i></td><td>NPx acceleration enabled.</td></tr></table>	Option	Description	<i>none</i>	NPx acceleration disabled.	<i>basic</i>	NPx acceleration enabled.			
	Option	Description								
	<i>none</i>	NPx acceleration disabled.								
<i>basic</i>	NPx acceleration enabled.									
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 128 Maximum value: 4096							
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-	heuristic						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>accurate</i>	Accurately count concurrent sessions, demands more resources.		
	<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.		
socket-size	IPS socket buffer size. Max and default value depend on available memory. Can be changed to tune performance.	integer	Minimum value: 128 ** 0 Maximum value: 256 **	
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of kernel session TTL for IPS sessions.		
	<i>disable</i>	Disable use of kernel session TTL for IPS sessions.		
traffic-submit	Enable/disable submitting attack data found by this FortiGate to FortiGuard.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable traffic submit.		
	<i>disable</i>	Disable traffic submit.		

* This parameter may not exist in some models.

** Values may differ between models.

config tls-active-probe

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		

Parameter	Description	Type	Size	Default
source-ip	Source IP address used for TLS active probe.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used for TLS active probe.	ipv6-address	Not Specified	::
vdom	Virtual domain name for TLS active probe.	string	Maximum length: 31	

config ips rule

Configure IPS rules. Read-only.

```

config ips rule
  Description: Configure IPS rules. Read-only.
  edit <name>
    set action [pass|block]
    set application {user}
    set date {integer}
    set group {string}
    set location {user}
    set log [disable|enable]
    set log-packet [disable|enable]
    config metadata
      Description: Meta data. Read-only.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
    set os {user}
    set rev {integer}
    set rule-id {integer}
    set service {user}
    set severity {user}
  next
end

```

config ips rule

Parameter	Description	Type	Size	Default
action	Action. Read-only.	option	-	pass

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Pass or allow matching traffic.</td></tr><tr><td><i>block</i></td><td>Block or drop matching traffic.</td></tr></table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.			
	Option	Description								
	<i>pass</i>	Pass or allow matching traffic.								
<i>block</i>	Block or drop matching traffic.									
application	Vulnerable applications. Read-only.	user	Not Specified							
date	Date. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							
group	Group. Read-only.	string	Maximum length: 63							
location	Vulnerable location. Read-only.	user	Not Specified							
log	Enable/disable logging. Read-only.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.			
	Option	Description								
	<i>disable</i>	Disable logging.								
<i>enable</i>	Enable logging.									
log-packet	Enable/disable packet logging. Read-only.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet logging.</td></tr><tr><td><i>enable</i></td><td>Enable packet logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable packet logging.	<i>enable</i>	Enable packet logging.			
	Option	Description								
	<i>disable</i>	Disable packet logging.								
<i>enable</i>	Enable packet logging.									
name	Rule name.	string	Maximum length: 63							
os	Vulnerable operation systems. Read-only.	user	Not Specified							
rev	Revision. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							
rule-id	Rule ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							
service	Vulnerable service. Read-only.	user	Not Specified							
severity	Severity. Read-only.	user	Not Specified							

config metadata

Parameter	Description	Type	Size	Default
id	ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
metaid	Meta ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
valueid	Value ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

config ips rule-settings

Configure IPS rule setting. Read-only.

```
config ips rule-settings
  Description: Configure IPS rule setting. Read-only.
  edit <id>
  next
end
```

config ips rule-settings

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

config ips sensor

Configure IPS sensor.

```
config ips sensor
  Description: Configure IPS sensor.
  edit <name>
    set block-malicious-url [disable|enable]
```

```

set comment {var-string}
config entries
    Description: IPS sensor filter.
    edit <id>
        set action [pass|block|...]
        set application {user}
        set cve <cve-entry1>, <cve-entry2>, ...
        set default-action [all|pass|...]
        set default-status [all|enable|...]
        config exempt-ip
            Description: Traffic from selected source or destination IP addresses is
exempt from this signature.
            edit <id>
                set dst-ip {ipv4-classnet}
                set src-ip {ipv4-classnet}
            next
        end
        set last-modified {user}
        set location {user}
        set log [disable|enable]
        set log-attack-context [disable|enable]
        set log-packet [disable|enable]
        set os {user}
        set protocol {user}
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set rate-count {integer}
        set rate-duration {integer}
        set rate-mode [periodical|continuous]
        set rate-track [none|src-ip|...]
        set rule <id1>, <id2>, ...
        set severity {user}
        set status [disable|enable|...]
        set vuln-type <id1>, <id2>, ...
    next
end
set extended-log [enable|disable]
set replacemsg-group {string}
set scan-botnet-connections [disable|block|...]
next
end

```

config ips sensor

Parameter	Description	Type	Size	Default
block-malicious-url	Enable/disable malicious URL blocking.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable malicious URL blocking.		
	<i>enable</i>	Enable malicious URL blocking.		
comment	Comment.	var-string	Maximum length: 255	
extended-log	Enable/disable extended logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
name	Sensor name.	string	Maximum length: 47	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not scan connections to botnet servers.		
	<i>block</i>	Block connections to botnet servers.		
	<i>monitor</i>	Log connections to botnet servers.		

config entries

Parameter	Description	Type	Size	Default
action	Action taken with traffic in which signatures are detected.	option	-	default
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
	<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.		

Parameter	Description	Type	Size	Default								
application	Operating systems to be protected. Use all for every application and other for unlisted application.	user	Not Specified	all								
cve <cve-entry>	List of CVE IDs of the signatures to add to the sensor. CVE IDs or CVE wildcards.	string	Maximum length: 19									
default-action	Signature default action filter.	option	-	all								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Selects signatures with any default action.</td></tr><tr><td>pass</td><td>Selects signatures with default action 'pass'.</td></tr><tr><td>block</td><td>Selects signatures with default action 'block'.</td></tr></table>	Option	Description	all	Selects signatures with any default action.	pass	Selects signatures with default action 'pass'.	block	Selects signatures with default action 'block'.			
Option	Description											
all	Selects signatures with any default action.											
pass	Selects signatures with default action 'pass'.											
block	Selects signatures with default action 'block'.											
default-status	Signature default status filter.	option	-	all								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Selects signatures with any default status.</td></tr><tr><td>enable</td><td>Selects signatures enabled by default.</td></tr><tr><td>disable</td><td>Selects signatures disabled by default.</td></tr></table>	Option	Description	all	Selects signatures with any default status.	enable	Selects signatures enabled by default.	disable	Selects signatures disabled by default.			
Option	Description											
all	Selects signatures with any default status.											
enable	Selects signatures enabled by default.											
disable	Selects signatures disabled by default.											
id	Rule ID in IPS database (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295									
last-modified	Filter by signature last modified date. Formats: before <date>, after <date>, between <start-date> <end-date>.	user	Not Specified									
location	Protect client or server traffic.	user	Not Specified	all								
log	Enable/disable logging of signatures included in filter.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of selected rules.</td></tr><tr><td>enable</td><td>Enable logging of selected rules.</td></tr></table>	Option	Description	disable	Disable logging of selected rules.	enable	Enable logging of selected rules.					
Option	Description											
disable	Disable logging of selected rules.											
enable	Enable logging of selected rules.											
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of detailed attack context.</td></tr><tr><td><i>enable</i></td><td>Enable logging of detailed attack context.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of detailed attack context.	<i>enable</i>	Enable logging of detailed attack context.			
	Option	Description								
	<i>disable</i>	Disable logging of detailed attack context.								
<i>enable</i>	Enable logging of detailed attack context.									
log-packet	Enable/disable packet logging. Enable to save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet logging of selected rules.</td></tr><tr><td><i>enable</i></td><td>Enable packet logging of selected rules.</td></tr></table>	Option	Description	<i>disable</i>	Disable packet logging of selected rules.	<i>enable</i>	Enable packet logging of selected rules.			
	Option	Description								
	<i>disable</i>	Disable packet logging of selected rules.								
<i>enable</i>	Enable packet logging of selected rules.									
os	Operating systems to be protected. Use all for every operating system and other for unlisted operating systems.	user	Not Specified	all						
protocol	Protocols to be examined. Use all for every protocol and other for unlisted protocols.	user	Not Specified	all						
quarantine	Quarantine method.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Quarantine is disabled.</td></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
	Option	Description								
	<i>none</i>	Quarantine is disabled.								
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. (Format <i>###d##h##m</i> , minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine logging.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
	Option	Description								
	<i>disable</i>	Disable quarantine logging.								
<i>enable</i>	Enable quarantine logging.									
rate-count	Count of the rate.	integer	Minimum value: 0 0 Maximum value: 65535	0						

Parameter	Description	Type	Size	Default												
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60												
rate-mode	Rate limit mode.	option	-	continuous												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>periodical</i></td><td>Allow configured number of packets every rate-duration.</td></tr><tr><td><i>continuous</i></td><td>Block packets once the rate is reached.</td></tr></table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.									
Option	Description															
<i>periodical</i>	Allow configured number of packets every rate-duration.															
<i>continuous</i>	Block packets once the rate is reached.															
rate-track	Track the packet protocol field.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>none</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr><tr><td><i>dhcp-client-mac</i></td><td>DHCP client.</td></tr><tr><td><i>dns-domain</i></td><td>DNS domain.</td></tr></table>	Option	Description	<i>none</i>	none	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.	<i>dhcp-client-mac</i>	DHCP client.	<i>dns-domain</i>	DNS domain.			
Option	Description															
<i>none</i>	none															
<i>src-ip</i>	Source IP.															
<i>dest-ip</i>	Destination IP.															
<i>dhcp-client-mac</i>	DHCP client.															
<i>dns-domain</i>	DNS domain.															
rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295													
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	all												
status	Status of the signatures included in filter. Only those filters with a status to enable are used.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status of selected rules.</td></tr><tr><td><i>enable</i></td><td>Enable status of selected rules.</td></tr><tr><td><i>default</i></td><td>Default.</td></tr></table>	Option	Description	<i>disable</i>	Disable status of selected rules.	<i>enable</i>	Enable status of selected rules.	<i>default</i>	Default.							
Option	Description															
<i>disable</i>	Disable status of selected rules.															
<i>enable</i>	Enable status of selected rules.															
<i>default</i>	Default.															
vuln-type <id>	List of signature vulnerability types to filter by. Vulnerability type ID.	integer	Minimum value: 0 Maximum value: 4294967295													

config exempt-ip

Parameter	Description	Type	Size	Default
dst-ip	Destination IP address and netmask (applies to packet matching the signature).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
id	Exempt IP ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
src-ip	Source IP address and netmask (applies to packet matching the signature).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config ips settings

Configure IPS VDOM parameter.

```
config ips settings
  Description: Configure IPS VDOM parameter.
  set ha-session-pickup [connectivity|security]
  set ips-packet-quota {integer}
  set packet-log-history {integer}
  set packet-log-memory {integer}
  set packet-log-post-attack {integer}
  set proxy-inline-ips [disable|enable]
end
```

config ips settings

Parameter	Description	Type	Size	Default						
ha-session-pickup	IPS HA failover session pickup preference.	option	-	connectivity						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>connectivity</td><td>Prefer session continuity.</td></tr><tr><td>security</td><td>Prefer session complete security.</td></tr></table>	Option	Description	connectivity	Prefer session continuity.	security	Prefer session complete security.			
Option	Description									
connectivity	Prefer session continuity.									
security	Prefer session complete security.									
ips-packet-quota	Maximum amount of disk space in MB for logged packets when logging to disk. Range depends on disk size.	integer	Minimum value: 0 0 Maximum value: 4294967295							
packet-log-history	Number of packets to capture before and including the one in which the IPS signature is detected (1 - 255).	integer	Minimum value: 1 1 Maximum value: 255							

Parameter	Description	Type	Size	Default						
packet-log-memory	Maximum memory can be used by packet log (64 - 8192 kB).	integer	Minimum value: 64 Maximum value: 8192	256						
packet-log-post-attack	Number of packets to log after the IPS signature is detected (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0						
proxy-inline-ips	Enable/disable proxy-mode policy inline IPS support.	option	-	enable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not allow inline IPS in proxy-mode policy.</td></tr><tr><td>enable</td><td>Allow inline IPS in proxy-mode policy.</td></tr></table>	Option	Description	disable	Do not allow inline IPS in proxy-mode policy.	enable	Allow inline IPS in proxy-mode policy.			
Option	Description									
disable	Do not allow inline IPS in proxy-mode policy.									
enable	Allow inline IPS in proxy-mode policy.									

** Values may differ between models.

config ips view-map

Configure IPS view-map. Read-only.

```
config ips view-map
  Description: Configure IPS view-map. Read-only.
  edit <id>
    set id-policy-id {integer}
    set policy-id {integer}
    set vdom-id {integer}
    set which [firewall|interface|...]
  next
end
```

config ips view-map

Parameter	Description	Type	Size	Default
id	View ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
id-policy-id	ID-based policy ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
policy-id	Policy ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
vdom-id	VDOM ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
which	Policy. Read-only.	option	-	firewall
	Option	Description		
	<i>firewall</i>	Firewall policy.		
	<i>interface</i>	Interface policy.		
	<i>interface6</i>	Interface policy6.		
	<i>sniffer</i>	Sniffer policy.		
	<i>sniffer6</i>	Sniffer policy6.		
	<i>explicit</i>	explicit proxy policy.		

log

This section includes syntax for the following commands:

- [config log azure-security-center2 filter on page 772](#)
- [config log azure-security-center2 setting on page 776](#)
- [config log azure-security-center filter on page 766](#)
- [config log azure-security-center setting on page 770](#)
- [config log custom-field on page 778](#)
- [config log disk filter on page 778](#)
- [config log disk setting on page 782](#)
- [config log eventfilter on page 788](#)
- [config log fortianalyzer-cloud filter on page 843](#)
- [config log fortianalyzer-cloud override-filter on page 847](#)
- [config log fortianalyzer-cloud override-setting on page 851](#)
- [config log fortianalyzer-cloud setting on page 852](#)
- [config log fortianalyzer2 filter on page 808](#)
- [config log fortianalyzer2 override-filter on page 812](#)
- [config log fortianalyzer2 override-setting on page 816](#)
- [config log fortianalyzer2 setting on page 821](#)
- [config log fortianalyzer3 filter on page 826](#)
- [config log fortianalyzer3 override-filter on page 830](#)
- [config log fortianalyzer3 override-setting on page 834](#)
- [config log fortianalyzer3 setting on page 839](#)
- [config log fortianalyzer filter on page 791](#)
- [config log fortianalyzer override-filter on page 795](#)
- [config log fortianalyzer override-setting on page 799](#)
- [config log fortianalyzer setting on page 804](#)
- [config log fortiguard filter on page 856](#)
- [config log fortiguard override-filter on page 860](#)
- [config log fortiguard override-setting on page 863](#)
- [config log fortiguard setting on page 865](#)
- [config log gui-display on page 868](#)
- [config log memory filter on page 869](#)
- [config log memory global-setting on page 873](#)
- [config log memory setting on page 874](#)
- [config log null-device filter on page 874](#)
- [config log null-device setting on page 878](#)
- [config log setting on page 879](#)
- [config log syslogd2 filter on page 900](#)

-
- [config log syslogd2 override-filter on page 904](#)
 - [config log syslogd2 override-setting on page 908](#)
 - [config log syslogd2 setting on page 913](#)
 - [config log syslogd3 filter on page 917](#)
 - [config log syslogd3 override-filter on page 921](#)
 - [config log syslogd3 override-setting on page 925](#)
 - [config log syslogd3 setting on page 929](#)
 - [config log syslogd4 filter on page 933](#)
 - [config log syslogd4 override-filter on page 937](#)
 - [config log syslogd4 override-setting on page 941](#)
 - [config log syslogd4 setting on page 946](#)
 - [config log syslogd filter on page 884](#)
 - [config log syslogd override-filter on page 888](#)
 - [config log syslogd override-setting on page 892](#)
 - [config log syslogd setting on page 896](#)
 - [config log tacacs+accounting2 filter on page 952](#)
 - [config log tacacs+accounting2 setting on page 953](#)
 - [config log tacacs+accounting3 filter on page 954](#)
 - [config log tacacs+accounting3 setting on page 955](#)
 - [config log tacacs+accounting filter on page 950](#)
 - [config log tacacs+accounting setting on page 951](#)
 - [config log threat-weight on page 956](#)
 - [config log webtrends filter on page 967](#)
 - [config log webtrends setting on page 971](#)

config log azure-security-center filter



This command is available for model(s): FortiGate-VM64 Azure.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Filters for Azure Security Center.

```
config log azure-security-center filter
  Description: Filters for Azure Security Center.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
```

```
set ztna-traffic [enable|disable]
end
```

config log azure-security-center filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.					
Option	Description									
<i>enable</i>	Enable http transaction logging.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable VoIP logging.		
	<i>enable</i>	Enable ztna traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>gtp</i>	GTP log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		

Parameter	Description	Type	Size	Default						
filter	Free style filter string.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>				Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.
	Option	Description								
	include	Include logs that match the filter.								
exclude	Exclude logs that match the filter.									
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						

config log azure-security-center setting



This command is available for model(s): FortiGate-VM64 Azure.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Settings for Azure Security Center.

```
config log azure-security-center setting
  Description: Settings for Azure Security Center.
  set appliance-id {string}
  config custom-field-name
```

```

Description: Custom field name for CEF format logging.
edit <id>
    set custom {string}
    set name {string}
next
end
set eventhub-name {string}
set policy-name {string}
set policy-saskey {string}
set servicebus-namespace {string}
set status [enable|disable]
end

```

config log azure-security-center setting

Parameter	Description	Type	Size	Default
appliance-id	Appliance ID.	string	Maximum length: 128	
eventhub-name	Event hub name.	string	Maximum length: 128	
policy-name	Policy name.	string	Maximum length: 128	
policy-saskey	Policy saskey.	string	Maximum length: 128	
servicebus-namespace	Service bus namespace.	string	Maximum length: 128	
status	Enable Azure Security Center logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log azure-security-center2 filter



This command is available for model(s): FortiGate-VM64 Azure.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Filters for Azure Security Center.

```
config log azure-security-center2 filter
  Description: Filters for Azure Security Center.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
```

```

set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log azure-security-center2 filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable anomaly logging.</td></tr><tr><td>disable</td><td>Disable anomaly logging.</td></tr></table>	Option	Description	enable	Enable anomaly logging.	disable	Disable anomaly logging.			
Option	Description									
enable	Enable anomaly logging.									
disable	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Debug logging.</td></tr><tr><td>disable</td><td>Disable Debug logging.</td></tr></table>	Option	Description	enable	Enable Debug logging.	disable	Disable Debug logging.			
Option	Description									
enable	Enable Debug logging.									
disable	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Forti-Switch logging.</td></tr><tr><td>disable</td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	enable	Enable Forti-Switch logging.	disable	Disable Forti-Switch logging.			
Option	Description									
enable	Enable Forti-Switch logging.									
disable	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable forward traffic logging.</td></tr><tr><td>disable</td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	enable	Enable forward traffic logging.	disable	Disable forward traffic logging.			
Option	Description									
enable	Enable forward traffic logging.									
disable	Disable forward traffic logging.									
gtp	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable GTP messages logging.</td></tr><tr><td>disable</td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	enable	Enable GTP messages logging.	disable	Disable GTP messages logging.			
Option	Description									
enable	Enable GTP messages logging.									
disable	Disable GTP messages logging.									

Parameter	Description	Type	Size	Default																		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.															
Option	Description																					
<i>enable</i>	Enable http transaction logging.																					
<i>disable</i>	Disable http transaction logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
voip	Enable/disable VoIP logging.	option	-	enable																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>gtp</i>	GTP log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>				Option	Description	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.
	Option	Description								
	<i>virtual-patch</i>	Virtual patch log.								
<i>debug</i>	Debug log.									
filter	Free style filter string.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>				Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.
	Option	Description								
	<i>include</i>	Include logs that match the filter.								
<i>exclude</i>	Exclude logs that match the filter.									
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							

config log azure-security-center2 setting



This command is available for model(s): FortiGate-VM64 Azure.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Settings for Azure Security Center.


```

config log azure-security-center2 setting
    Description: Settings for Azure Security Center.
    set appliance-id {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set eventhub-name {string}
    set policy-name {string}
    set policy-saskey {string}
    set servicebus-namespace {string}
    set status [enable|disable]
end

```

config log azure-security-center2 setting

Parameter	Description	Type	Size	Default
appliance-id	Appliance ID.	string	Maximum length: 128	
eventhub-name	Event hub name.	string	Maximum length: 128	
policy-name	Policy name.	string	Maximum length: 128	
policy-saskey	Policy saskey.	string	Maximum length: 128	
servicebus-namespace	Service bus namespace.	string	Maximum length: 128	
status	Enable Azure Security Center logging.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log custom-field

Configure custom log fields.

```
config log custom-field
    Description: Configure custom log fields.
    edit <id>
        set name {string}
        set value {string}
    next
end
```

config log custom-field

Parameter	Description	Type	Size	Default
id	Field ID string.	string	Maximum length: 35	
name	Field name (max: 15 characters).	string	Maximum length: 15	
value	Field value (max: 15 characters).	string	Maximum length: 15	

config log disk filter

Configure filters for local disk logging. Use these filters to determine the log messages to record according to severity and type.

```
config log disk filter
    Description: Configure filters for local disk logging. Use these filters to determine the log
    messages to record according to severity and type.
    set anomaly [enable|disable]
    set debug [enable|disable]
    set dlp-archive [enable|disable]
    set forti-switch [enable|disable]
```

```

set forward-traffic [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set http-transaction [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log disk filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
dlp-archive *	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.					
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable Forti-Switch logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Log to disk every message above and including this severity level.	option	-	information

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																																						
	<i>event</i>	Event log.																																						
	<i>virus</i>	Antivirus log.																																						
	<i>webfilter</i>	Web filter log.																																						
	<i>attack</i>	Attack log.																																						
	<i>spam</i>	Antispam log.																																						
	<i>anomaly</i>	Anomaly log.																																						
	<i>voip</i>	VoIP log.																																						
	<i>dlp</i>	DLP log.																																						
	<i>app-ctrl</i>	Application control log.																																						
	<i>waf</i>	Web application firewall log.																																						
	<i>dns</i>	DNS detail log.																																						
	<i>ssh</i>	SSH log.																																						
	<i>ssl</i>	SSL log.																																						
	<i>file-filter</i>	File filter log.																																						
	<i>icap</i>	ICAP log.																																						
	<i>virtual-patch</i>	Virtual patch log.																																						
<i>debug</i>	Debug log.																																							
filter	Free style filter string.	string	Maximum length: 1023																																					
filter-type	Include/exclude logs that match the filter.	option	-	include																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																																	
	Option	Description																																						
	<i>include</i>	Include logs that match the filter.																																						
<i>exclude</i>	Exclude logs that match the filter.																																							
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295																																					

config log disk setting

Settings for local disk logging.

```

config log disk setting
    Description: Settings for local disk logging.
    set diskfull [overwrite|nolog]
    set dlp-archive-quota {integer}
    set full-final-warning-threshold {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set log-quota {integer}
    set max-log-file-size {integer}
    set max-policy-packet-capture-size {integer}
    set maximum-log-age {integer}
    set report-quota {integer}
    set roll-day {option1}, {option2}, ...
    set roll-schedule [daily|weekly]
    set roll-time {user}
    set source-ip {ipv4-address}
    set status [enable|disable]
    set upload [enable|disable]
    set upload-delete-files [enable|disable]
    set upload-destination {option}
    set upload-ssl-conn [default|high|...]
    set uploadaddir {string}
    set uploadip {ipv4-address}
    set uploadpass {password}
    set uploadport {integer}
    set uploadsched [disable|enable]
    set uploadtime {user}
    set uploadtype {option1}, {option2}, ...
    set uploaduser {string}
    set vrf-select {integer}
end

```

config log disk setting

Parameter	Description	Type	Size	Default						
diskfull	Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full (default = overwrite).	option	-	overwrite						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>overwrite</i></td><td>Overwrite the oldest logs when the log disk is full.</td></tr><tr><td><i>nolog</i></td><td>Stop logging when the log disk is full.</td></tr></table>				Option	Description	<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.	<i>nolog</i>	Stop logging when the log disk is full.
Option	Description									
<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.									
<i>nolog</i>	Stop logging when the log disk is full.									

Parameter	Description	Type	Size	Default								
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 0 Maximum value: 4294967295									
full-final-warning-threshold	Log full final warning threshold as a percent (3 - 100, default = 95).	integer	Minimum value: 95 3 Maximum value: 100									
full-first-warning-threshold	Log full first warning threshold as a percent (1 - 98, default = 75).	integer	Minimum value: 75 1 Maximum value: 98									
full-second-warning-threshold	Log full second warning threshold as a percent (2 - 99, default = 90).	integer	Minimum value: 90 2 Maximum value: 99									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPS packet archiving.</td></tr><tr><td>disable</td><td>Disable IPS packet archiving.</td></tr></table>				Option	Description	enable	Enable IPS packet archiving.	disable	Disable IPS packet archiving.		
Option	Description											
enable	Enable IPS packet archiving.											
disable	Disable IPS packet archiving.											
log-quota	Disk log quota (MB).	integer	Minimum value: 0 0 Maximum value: 4294967295									
max-log-file-size	Maximum log file size before rolling (1 - 100 Mbytes).	integer	Minimum value: 20 1 Maximum value: 100									

Parameter	Description	Type	Size	Default																
max-policy-packet-capture-size	Maximum size of policy sniffer in MB (0 means unlimited).	integer	Minimum value: 0 Maximum value: 4294967295	100																
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650	7																
report-quota *	Report db quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0																
roll-day	Day of week on which to roll log file.	option	-	sunday																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday</td></tr><tr><td><i>monday</i></td><td>Monday</td></tr><tr><td><i>tuesday</i></td><td>Tuesday</td></tr><tr><td><i>wednesday</i></td><td>Wednesday</td></tr><tr><td><i>thursday</i></td><td>Thursday</td></tr><tr><td><i>friday</i></td><td>Friday</td></tr><tr><td><i>saturday</i></td><td>Saturday</td></tr></table>				Option	Description	<i>sunday</i>	Sunday	<i>monday</i>	Monday	<i>tuesday</i>	Tuesday	<i>wednesday</i>	Wednesday	<i>thursday</i>	Thursday	<i>friday</i>	Friday	<i>saturday</i>	Saturday
Option	Description																			
<i>sunday</i>	Sunday																			
<i>monday</i>	Monday																			
<i>tuesday</i>	Tuesday																			
<i>wednesday</i>	Wednesday																			
<i>thursday</i>	Thursday																			
<i>friday</i>	Friday																			
<i>saturday</i>	Saturday																			
roll-schedule	Frequency to check log file for rolling.	option	-	daily																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>daily</i></td><td>Check the log file once a day.</td></tr><tr><td><i>weekly</i></td><td>Check the log file once a week.</td></tr></table>				Option	Description	<i>daily</i>	Check the log file once a day.	<i>weekly</i>	Check the log file once a week.										
Option	Description																			
<i>daily</i>	Check the log file once a day.																			
<i>weekly</i>	Check the log file once a week.																			
roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified																	
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified	0.0.0.0																
status	Enable/disable local disk logging.	option	-	disable **																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log to local disk.</td></tr><tr><td><i>disable</i></td><td>Do not log to local disk.</td></tr></table>				Option	Description	<i>enable</i>	Log to local disk.	<i>disable</i>	Do not log to local disk.										
Option	Description																			
<i>enable</i>	Log to local disk.																			
<i>disable</i>	Do not log to local disk.																			

Parameter	Description	Type	Size	Default										
upload	Enable/disable uploading log files when they are rolled.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable uploading log files when they are rolled.</td></tr><tr><td><i>disable</i></td><td>Disable uploading log files when they are rolled.</td></tr></table>	Option	Description	<i>enable</i>	Enable uploading log files when they are rolled.	<i>disable</i>	Disable uploading log files when they are rolled.							
Option	Description													
<i>enable</i>	Enable uploading log files when they are rolled.													
<i>disable</i>	Disable uploading log files when they are rolled.													
upload-delete-files	Delete log files after uploading (default = enable).	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Delete log files after uploading.</td></tr><tr><td><i>disable</i></td><td>Do not delete log files after uploading.</td></tr></table>	Option	Description	<i>enable</i>	Delete log files after uploading.	<i>disable</i>	Do not delete log files after uploading.							
Option	Description													
<i>enable</i>	Delete log files after uploading.													
<i>disable</i>	Do not delete log files after uploading.													
upload-destination	The type of server to upload log files to. Only FTP is currently supported.	option	-	ftp-server										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ftp-server</i></td><td>Upload rolled log files to an FTP server.</td></tr></table>	Option	Description	<i>ftp-server</i>	Upload rolled log files to an FTP server.									
Option	Description													
<i>ftp-server</i>	Upload rolled log files to an FTP server.													
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-	default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>FTPS with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>FTPS with high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>FTPS with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable FTPS communication.</td></tr></table>	Option	Description	<i>default</i>	FTPS with high and medium encryption algorithms.	<i>high</i>	FTPS with high encryption algorithms.	<i>low</i>	FTPS with low encryption algorithms.	<i>disable</i>	Disable FTPS communication.			
Option	Description													
<i>default</i>	FTPS with high and medium encryption algorithms.													
<i>high</i>	FTPS with high encryption algorithms.													
<i>low</i>	FTPS with low encryption algorithms.													
<i>disable</i>	Disable FTPS communication.													
uploaddir	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63											
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified	0.0.0.0										
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified											
uploadport	TCP port to use for communicating with the FTP server (default = 21).	integer	Minimum value: 0 Maximum value: 65535	21										

Parameter	Description	Type	Size	Default																														
uploadsched	Set the schedule for uploading log files to the FTP server (default = disable = upload when rolling).	option	-	disable																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Upload when rolling.</td></tr><tr><td>enable</td><td>Scheduled upload.</td></tr></table>	Option	Description	disable	Upload when rolling.	enable	Scheduled upload.																											
Option	Description																																	
disable	Upload when rolling.																																	
enable	Scheduled upload.																																	
uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified																															
uploadtype	Types of log files to upload. Separate multiple entries with a space.	option	-	traffic event virus webfilter IPS emailfilter dlp-archive anomaly voip dlp app-ctrl waf dns ssh ssl **																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Upload traffic log.</td></tr><tr><td>event</td><td>Upload event log.</td></tr><tr><td>virus</td><td>Upload anti-virus log.</td></tr><tr><td>webfilter</td><td>Upload web filter log.</td></tr><tr><td>IPS</td><td>Upload IPS log.</td></tr><tr><td>emailfilter</td><td>Upload spam filter log.</td></tr><tr><td>dlp-archive</td><td>Upload DLP archive.</td></tr><tr><td>anomaly</td><td>Upload anomaly log.</td></tr><tr><td>voip</td><td>Upload VoIP log.</td></tr><tr><td>dlp</td><td>Upload DLP log.</td></tr><tr><td>app-ctrl</td><td>Upload application control log.</td></tr><tr><td>waf</td><td>Upload web application firewall log.</td></tr><tr><td>dns</td><td>Upload DNS log.</td></tr><tr><td>ssh</td><td>Upload SSH log.</td></tr></table>	Option	Description	traffic	Upload traffic log.	event	Upload event log.	virus	Upload anti-virus log.	webfilter	Upload web filter log.	IPS	Upload IPS log.	emailfilter	Upload spam filter log.	dlp-archive	Upload DLP archive.	anomaly	Upload anomaly log.	voip	Upload VoIP log.	dlp	Upload DLP log.	app-ctrl	Upload application control log.	waf	Upload web application firewall log.	dns	Upload DNS log.	ssh	Upload SSH log.			
Option	Description																																	
traffic	Upload traffic log.																																	
event	Upload event log.																																	
virus	Upload anti-virus log.																																	
webfilter	Upload web filter log.																																	
IPS	Upload IPS log.																																	
emailfilter	Upload spam filter log.																																	
dlp-archive	Upload DLP archive.																																	
anomaly	Upload anomaly log.																																	
voip	Upload VoIP log.																																	
dlp	Upload DLP log.																																	
app-ctrl	Upload application control log.																																	
waf	Upload web application firewall log.																																	
dns	Upload DNS log.																																	
ssh	Upload SSH log.																																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	Upload SSL log.		
	<i>file-filter</i>	Upload file-filter log.		
	<i>icap</i>	Upload ICAP log.		
	<i>virtual-patch</i>	Upload virtual-patch log.		
	<i>debug</i>	Upload debug log.		
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	

* This parameter may not exist in some models.

** Values may differ between models.

config log eventfilter

Configure log event filters.

```

config log eventfilter
  Description: Configure log event filters.
  set cifs [enable|disable]
  set connector [enable|disable]
  set endpoint [enable|disable]
  set event [enable|disable]
  set fortiextender [enable|disable]
  set ha [enable|disable]
  set rest-api [enable|disable]
  set router [enable|disable]
  set sdwan [enable|disable]
  set security-rating [enable|disable]
  set switch-controller [enable|disable]
  set system [enable|disable]
  set user [enable|disable]
  set vpn [enable|disable]
  set wan-opt [enable|disable]
  set webproxy [enable|disable]
  set wireless-activity [enable|disable]
end

```

config log eventfilter

Parameter	Description	Type	Size	Default
cifs	Enable/disable CIFS logging.	option	-	enable
	Option	Description		
	enable	Enable CIFS logging.		
	disable	Disable CIFS logging.		
connector	Enable/disable SDN connector logging.	option	-	enable
	Option	Description		
	enable	Enable SDN connector logging.		
	disable	Disable SDN connector logging.		
endpoint	Enable/disable endpoint event logging.	option	-	enable
	Option	Description		
	enable	Enable endpoint event logging.		
	disable	Disable endpoint event logging.		
event	Enable/disable event logging.	option	-	enable
	Option	Description		
	enable	Enable event logging.		
	disable	Disable event logging.		
fortiextender	Enable/disable FortiExtender logging.	option	-	enable
	Option	Description		
	enable	Enable Forti-Extender logging.		
	disable	Disable Forti-Extender logging.		
ha	Enable/disable ha event logging.	option	-	enable
	Option	Description		
	enable	Enable ha event logging.		
	disable	Disable ha event logging.		
rest-api	Enable/disable REST API logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable REST API logging.		
	<i>disable</i>	Disable REST API logging.		
router	Enable/disable router event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable router event logging.		
	<i>disable</i>	Disable router event logging.		
sdwan	Enable/disable SD-WAN logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable SD-WAN logging.		
	<i>disable</i>	Disable SD-WAN logging.		
security-rating	Enable/disable Security Rating result logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Security Fabric audit result logging.		
	<i>disable</i>	Disable Security Fabric audit result logging.		
switch-controller	Enable/disable Switch-Controller logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		
system	Enable/disable system event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable system event logging.		
	<i>disable</i>	Disable system event logging.		
user	Enable/disable user authentication event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable user authentication event logging.		
	<i>disable</i>	Disable user authentication event logging.		

Parameter	Description	Type	Size	Default						
vpn	Enable/disable VPN event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable VPN event logging.</td></tr><tr><td>disable</td><td>Disable VPN event logging.</td></tr></table>	Option	Description	enable	Enable VPN event logging.	disable	Disable VPN event logging.			
Option	Description									
enable	Enable VPN event logging.									
disable	Disable VPN event logging.									
wan-opt	Enable/disable WAN optimization event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WAN optimization event logging.</td></tr><tr><td>disable</td><td>Disable WAN optimization event logging.</td></tr></table>	Option	Description	enable	Enable WAN optimization event logging.	disable	Disable WAN optimization event logging.			
Option	Description									
enable	Enable WAN optimization event logging.									
disable	Disable WAN optimization event logging.									
webproxy *	Enable/disable web proxy event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Web Proxy event logging.</td></tr><tr><td>disable</td><td>Disable Web Proxy event logging.</td></tr></table>	Option	Description	enable	Enable Web Proxy event logging.	disable	Disable Web Proxy event logging.			
Option	Description									
enable	Enable Web Proxy event logging.									
disable	Disable Web Proxy event logging.									
wireless-activity	Enable/disable wireless event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable wireless event logging.</td></tr><tr><td>disable</td><td>Disable wireless event logging.</td></tr></table>	Option	Description	enable	Enable wireless event logging.	disable	Disable wireless event logging.			
Option	Description									
enable	Enable wireless event logging.									
disable	Disable wireless event logging.									

* This parameter may not exist in some models.

config log fortianalyzer filter

Filters for FortiAnalyzer.

```

config log fortianalyzer filter
  Description: Filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
    end
  end
end

```

```

        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set http-transaction [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log fortianalyzer filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																												
	<i>anomaly</i>	Anomaly log.																												
	<i>voip</i>	VoIP log.																												
	<i>dlp</i>	DLP log.																												
	<i>app-ctrl</i>	Application control log.																												
	<i>waf</i>	Web application firewall log.																												
	<i>dns</i>	DNS detail log.																												
	<i>ssh</i>	SSH log.																												
	<i>ssl</i>	SSL log.																												
	<i>file-filter</i>	File filter log.																												
	<i>icap</i>	ICAP log.																												
	<i>virtual-patch</i>	Virtual patch log.																												
<i>debug</i>	Debug log.																													
filter	Free style filter string.	string	Maximum length: 1023																											
filter-type	Include/exclude logs that match the filter.	option	-	include																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																							
	Option	Description																												
	<i>include</i>	Include logs that match the filter.																												
<i>exclude</i>	Exclude logs that match the filter.																													
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295																											

config log fortianalyzer override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer override-filter
  Description: Override filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
```

```

config free-style
  Description: Free style filters.
  edit <id>
    set category [traffic|event|...]
    set filter {string}
    set filter-type [include|exclude]
  next
end
set gtp [enable|disable]
set http-transaction [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log fortianalyzer override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable anomaly logging.</td></tr><tr><td>disable</td><td>Disable anomaly logging.</td></tr></table>	Option	Description	enable	Enable anomaly logging.	disable	Disable anomaly logging.			
Option	Description									
enable	Enable anomaly logging.									
disable	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Debug logging.</td></tr><tr><td>disable</td><td>Disable Debug logging.</td></tr></table>	Option	Description	enable	Enable Debug logging.	disable	Disable Debug logging.			
Option	Description									
enable	Enable Debug logging.									
disable	Disable Debug logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DLP archive logging.</td></tr><tr><td>disable</td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	enable	Enable DLP archive logging.	disable	Disable DLP archive logging.			
Option	Description									
enable	Enable DLP archive logging.									
disable	Disable DLP archive logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Forti-Switch logging.</td></tr><tr><td>disable</td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	enable	Enable Forti-Switch logging.	disable	Disable Forti-Switch logging.			
Option	Description									
enable	Enable Forti-Switch logging.									
disable	Disable Forti-Switch logging.									

Parameter	Description	Type	Size	Default								
forward-traffic	Enable/disable forward traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.					
Option	Description											
<i>enable</i>	Enable forward traffic logging.											
<i>disable</i>	Disable forward traffic logging.											
gtp *	Enable/disable GTP messages logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.					
Option	Description											
<i>enable</i>	Enable GTP messages logging.											
<i>disable</i>	Disable GTP messages logging.											
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.					
Option	Description											
<i>enable</i>	Enable http transaction logging.											
<i>disable</i>	Disable http transaction logging.											
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.					
Option	Description											
<i>enable</i>	Enable local in or out traffic logging.											
<i>disable</i>	Disable local in or out traffic logging.											
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.					
Option	Description											
<i>enable</i>	Enable multicast traffic logging.											
<i>disable</i>	Disable multicast traffic logging.											
severity	Lowest severity level to log.	option	-	information								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.			
Option	Description											
<i>emergency</i>	Emergency level.											
<i>alert</i>	Alert level.											
<i>critical</i>	Critical level.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																																
	<i>attack</i>	Attack log.																																
	<i>spam</i>	Antispam log.																																
	<i>anomaly</i>	Anomaly log.																																
	<i>voip</i>	VoIP log.																																
	<i>dlp</i>	DLP log.																																
	<i>app-ctrl</i>	Application control log.																																
	<i>waf</i>	Web application firewall log.																																
	<i>dns</i>	DNS detail log.																																
	<i>ssh</i>	SSH log.																																
	<i>ssl</i>	SSL log.																																
	<i>file-filter</i>	File filter log.																																
	<i>icap</i>	ICAP log.																																
	<i>virtual-patch</i>	Virtual patch log.																																
<i>debug</i>	Debug log.																																	
filter	Free style filter string.	string	Maximum length: 1023																															
filter-type	Include/exclude logs that match the filter.	option	-	include																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																											
	Option	Description																																
	<i>include</i>	Include logs that match the filter.																																
<i>exclude</i>	Exclude logs that match the filter.																																	
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																															

config log fortianalyzer override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer override-setting
  Description: Override FortiAnalyzer settings.
  set access-config [enable|disable]
  set alt-server {string}
```

```

set certificate {string}
set certificate-verification [enable|disable]
set conn-timeout {integer}
set enc-algorithm [high-medium|high|...]
set fallback-to-primary [enable|disable]
set hmac-algorithm {option}
set interface {string}
set interface-select-method [auto|sdwan|...]
set ips-archive [enable|disable]
set max-log-rate {integer}
set monitor-failure-retry-period {integer}
set monitor-keepalive-period {integer}
set preshared-key {string}
set priority [default|low]
set reliable [enable|disable]
set serial <name1>, <name2>, ...
set server {string}
set server-cert-ca {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
set use-management-vdom [enable|disable]
set vrf-select {integer}

```

end

config log fortianalyzer override-setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td>disable</td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>				Option	Description	enable	Enable FortiAnalyzer access to configuration and data.	disable	Disable FortiAnalyzer access to configuration and data.
Option	Description									
enable	Enable FortiAnalyzer access to configuration and data.									
disable	Disable FortiAnalyzer access to configuration and data.									
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127							
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.					
	Option	Description										
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.										
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.											
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
	Option	Description										
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
	<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.											
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td><i>disable</i></td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.					
	Option	Description										
	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.										
<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.							
	Option	Description										
<i>sha256</i>	Use SHA256 as HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											

Parameter	Description	Type	Size	Default						
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
Option	Description									
<i>enable</i>	Enable IPS packet archive logging.									
<i>disable</i>	Disable IPS packet archive logging.									
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5						
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5						
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63							
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.			
Option	Description									
<i>default</i>	Set FortiAnalyzer log transmission priority to default.									
<i>low</i>	Set FortiAnalyzer log transmission priority to low.									
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable reliable logging to FortiAnalyzer.									
<i>disable</i>	Disable reliable logging to FortiAnalyzer.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
server	The remote FortiAnalyzer.	string	Maximum length: 127							
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default														
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
status	Enable/disable logging to FortiAnalyzer.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.											
Option	Description																	
enable	Enable logging to FortiAnalyzer.																	
disable	Disable logging to FortiAnalyzer.																	
upload-day	Day of week (month) to upload logs.	user	Not Specified															
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.									
Option	Description																	
daily	Upload log files to FortiAnalyzer once a day.																	
weekly	Upload log files to FortiAnalyzer once a week.																	
monthly	Upload log files to FortiAnalyzer once a month.																	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.							
Option	Description																	
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.																	
realtime	Log directly to FortiAnalyzer in real time.																	
1-minute	Log directly to FortiAnalyzer at least every 1 minute.																	
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.																	

Parameter	Description	Type	Size	Default						
upload-time	Time to upload logs (hh:mm).	user	Not Specified							
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.
Option	Description									
<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config log fortianalyzer setting

Global FortiAnalyzer settings.

```

config log fortianalyzer setting
  Description: Global FortiAnalyzer settings.
  set access-config [enable|disable]
  set alt-server {string}
  set certificate {string}
  set certificate-verification [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
  set fallback-to-primary [enable|disable]
  set hmac-algorithm {option}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ips-archive [enable|disable]
  set max-log-rate {integer}
  set monitor-failure-retry-period {integer}
  set monitor-keepalive-period {integer}
  set preshared-key {string}
  set priority [default|low]
  set reliable [enable|disable]
  set serial <name1>, <name2>, ...
  set server {string}
  set server-cert-ca {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]

```

```

set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
set vrf-select {integer}
end

```

config log fortianalyzer setting

Parameter	Description	Type	Size	Default
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.		
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.		
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.		
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high
	Option	Description		
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.		
	<i>high</i>	Encrypt logs using high encryption algorithms.		
	<i>low</i>	Encrypt logs using all encryption algorithms.		
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td><i>disable</i></td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.					
	Option	Description										
	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.										
<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.							
	Option	Description										
<i>sha256</i>	Use SHA256 as HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.					
	Option	Description										
	<i>enable</i>	Enable IPS packet archive logging.										
<i>disable</i>	Disable IPS packet archive logging.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5								

Parameter	Description	Type	Size	Default														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63															
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	default	Set FortiAnalyzer log transmission priority to default.	low	Set FortiAnalyzer log transmission priority to low.											
Option	Description																	
default	Set FortiAnalyzer log transmission priority to default.																	
low	Set FortiAnalyzer log transmission priority to low.																	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable reliable logging to FortiAnalyzer.	disable	Disable reliable logging to FortiAnalyzer.											
Option	Description																	
enable	Enable reliable logging to FortiAnalyzer.																	
disable	Disable reliable logging to FortiAnalyzer.																	
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79															
server	The remote FortiAnalyzer.	string	Maximum length: 127															
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	

Parameter	Description	Type	Size	Default										
status	Enable/disable logging to FortiAnalyzer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>				Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.				
	Option	Description												
	enable	Enable logging to FortiAnalyzer.												
disable	Disable logging to FortiAnalyzer.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>				Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.		
	Option	Description												
	daily	Upload log files to FortiAnalyzer once a day.												
	weekly	Upload log files to FortiAnalyzer once a week.												
monthly	Upload log files to FortiAnalyzer once a month.													
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>				Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.
	Option	Description												
	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.												
	realtime	Log directly to FortiAnalyzer in real time.												
	1-minute	Log directly to FortiAnalyzer at least every 1 minute.												
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0										

config log fortianalyzer2 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer2 filter
  Description: Filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set debug [enable|disable]
```



```

set dlp-archive [enable|disable]
set forti-switch [enable|disable]
set forward-traffic [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set http-transaction [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log fortianalyzer2 filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
debug	Enable/disable debug logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Debug logging.		
	<i>disable</i>	Disable Debug logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Forti-Switch logging.		
	<i>disable</i>	Disable Forti-Switch logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Log every message above and including this severity level.	option	-	information

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																																						
	<i>event</i>	Event log.																																						
	<i>virus</i>	Antivirus log.																																						
	<i>webfilter</i>	Web filter log.																																						
	<i>attack</i>	Attack log.																																						
	<i>spam</i>	Antispam log.																																						
	<i>anomaly</i>	Anomaly log.																																						
	<i>voip</i>	VoIP log.																																						
	<i>dlp</i>	DLP log.																																						
	<i>app-ctrl</i>	Application control log.																																						
	<i>waf</i>	Web application firewall log.																																						
	<i>dns</i>	DNS detail log.																																						
	<i>ssh</i>	SSH log.																																						
	<i>ssl</i>	SSL log.																																						
	<i>file-filter</i>	File filter log.																																						
	<i>icap</i>	ICAP log.																																						
	<i>virtual-patch</i>	Virtual patch log.																																						
<i>debug</i>	Debug log.																																							
filter	Free style filter string.	string	Maximum length: 1023																																					
filter-type	Include/exclude logs that match the filter.	option	-	include																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																																	
	Option	Description																																						
	<i>include</i>	Include logs that match the filter.																																						
<i>exclude</i>	Exclude logs that match the filter.																																							
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295																																					

config log fortianalyzer2 override-filter

Override filters for FortiAnalyzer.

```

config log fortianalyzer2 override-filter
    Description: Override filters for FortiAnalyzer.
    set anomaly [enable|disable]
    set debug [enable|disable]
    set dlp-archive [enable|disable]
    set forti-switch [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set http-transaction [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

config log fortianalyzer2 override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									

Parameter	Description	Type	Size	Default						
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.			
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									
<i>disable</i>	Disable multicast traffic logging.									
severity	Log every message above and including this severity level.	option	-	information						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																																						
	<i>event</i>	Event log.																																						
	<i>virus</i>	Antivirus log.																																						
	<i>webfilter</i>	Web filter log.																																						
	<i>attack</i>	Attack log.																																						
	<i>spam</i>	Antispam log.																																						
	<i>anomaly</i>	Anomaly log.																																						
	<i>voip</i>	VoIP log.																																						
	<i>dlp</i>	DLP log.																																						
	<i>app-ctrl</i>	Application control log.																																						
	<i>waf</i>	Web application firewall log.																																						
	<i>dns</i>	DNS detail log.																																						
	<i>ssh</i>	SSH log.																																						
	<i>ssl</i>	SSL log.																																						
	<i>file-filter</i>	File filter log.																																						
	<i>icap</i>	ICAP log.																																						
	<i>virtual-patch</i>	Virtual patch log.																																						
<i>debug</i>	Debug log.																																							
filter	Free style filter string.	string	Maximum length: 1023																																					
filter-type	Include/exclude logs that match the filter.	option	-	include																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																																	
	Option	Description																																						
	<i>include</i>	Include logs that match the filter.																																						
<i>exclude</i>	Exclude logs that match the filter.																																							
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																																					

config log fortianalyzer2 override-setting

Override FortiAnalyzer settings.


```

config log fortianalyzer2 override-setting
    Description: Override FortiAnalyzer settings.
    set access-config [enable|disable]
    set alt-server {string}
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set fallback-to-primary [enable|disable]
    set hmac-algorithm {option}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set preshared-key {string}
    set priority [default|low]
    set reliable [enable|disable]
    set serial <name1>, <name2>, ...
    set server {string}
    set server-cert-ca {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
    set use-management-vdom [enable|disable]
    set vrf-select {integer}
end

```

config log fortianalyzer2 override-setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td>disable</td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>				Option	Description	enable	Enable FortiAnalyzer access to configuration and data.	disable	Disable FortiAnalyzer access to configuration and data.
Option	Description									
enable	Enable FortiAnalyzer access to configuration and data.									
disable	Disable FortiAnalyzer access to configuration and data.									
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127							
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default								
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td>disable</td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	enable	Enable identity verification of FortiAnalyzer by use of certificate.	disable	Disable identity verification of FortiAnalyzer by use of certificate.					
Option	Description											
enable	Enable identity verification of FortiAnalyzer by use of certificate.											
disable	Disable identity verification of FortiAnalyzer by use of certificate.											
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high-medium</td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td>high</td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td>low</td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	high-medium	Encrypt logs using high and medium encryption algorithms.	high	Encrypt logs using high encryption algorithms.	low	Encrypt logs using all encryption algorithms.			
Option	Description											
high-medium	Encrypt logs using high and medium encryption algorithms.											
high	Encrypt logs using high encryption algorithms.											
low	Encrypt logs using all encryption algorithms.											
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td>disable</td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	enable	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	disable	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.					
Option	Description											
enable	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
disable	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha256</td><td>Use SHA256 as HMAC algorithm.</td></tr></table>	Option	Description	sha256	Use SHA256 as HMAC algorithm.							
Option	Description											
sha256	Use SHA256 as HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.							
Option	Description											
auto	Set outgoing interface automatically.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description								
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.								
<i>specify</i>	Set outgoing interface manually.									
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
	Option	Description								
	<i>enable</i>	Enable IPS packet archive logging.								
<i>disable</i>	Disable IPS packet archive logging.									
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5						
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5						
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63							
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.			
	Option	Description								
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.								
<i>low</i>	Set FortiAnalyzer log transmission priority to low.									
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.			
	Option	Description								
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.								
<i>disable</i>	Disable reliable logging to FortiAnalyzer.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default														
server	The remote FortiAnalyzer.	string	Maximum length: 127															
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
status	Enable/disable logging to FortiAnalyzer.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.											
Option	Description																	
enable	Enable logging to FortiAnalyzer.																	
disable	Disable logging to FortiAnalyzer.																	
upload-day	Day of week (month) to upload logs.	user	Not Specified															
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.									
Option	Description																	
daily	Upload log files to FortiAnalyzer once a day.																	
weekly	Upload log files to FortiAnalyzer once a week.																	
monthly	Upload log files to FortiAnalyzer once a month.																	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>store-and-upload</i></td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td><i>realtime</i></td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td><i>1-minute</i></td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td><i>5-minute</i></td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
	Option	Description												
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.												
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.												
	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.												
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.							
	Option	Description												
	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.												
<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.													
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0										

config log fortianalyzer2 setting

Global FortiAnalyzer settings.

```

config log fortianalyzer2 setting
  Description: Global FortiAnalyzer settings.
  set access-config [enable|disable]
  set alt-server {string}
  set certificate {string}
  set certificate-verification [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
  set fallback-to-primary [enable|disable]
  set hmac-algorithm {option}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ips-archive [enable|disable]
  set max-log-rate {integer}
  set monitor-failure-retry-period {integer}

```

```

set monitor-keepalive-period {integer}
set preshared-key {string}
set priority [default|low]
set reliable [enable|disable]
set serial <name1>, <name2>, ...
set server {string}
set server-cert-ca {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
set vrf-select {integer}
end

```

config log fortianalyzer2 setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td>disable</td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	enable	Enable FortiAnalyzer access to configuration and data.	disable	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
enable	Enable FortiAnalyzer access to configuration and data.									
disable	Disable FortiAnalyzer access to configuration and data.									
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127							
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td>disable</td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	enable	Enable identity verification of FortiAnalyzer by use of certificate.	disable	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
enable	Enable identity verification of FortiAnalyzer by use of certificate.									
disable	Disable identity verification of FortiAnalyzer by use of certificate.									
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10						
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
	Option	Description										
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
	<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.											
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td><i>disable</i></td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.					
	Option	Description										
	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.										
<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.							
	Option	Description										
<i>sha256</i>	Use SHA256 as HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.					
	Option	Description										
	<i>enable</i>	Enable IPS packet archive logging.										
<i>disable</i>	Disable IPS packet archive logging.											

Parameter	Description	Type	Size	Default						
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5						
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5						
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63							
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>				Option	Description	default	Set FortiAnalyzer log transmission priority to default.	low	Set FortiAnalyzer log transmission priority to low.
Option	Description									
default	Set FortiAnalyzer log transmission priority to default.									
low	Set FortiAnalyzer log transmission priority to low.									
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>				Option	Description	enable	Enable reliable logging to FortiAnalyzer.	disable	Disable reliable logging to FortiAnalyzer.
Option	Description									
enable	Enable reliable logging to FortiAnalyzer.									
disable	Disable reliable logging to FortiAnalyzer.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
server	The remote FortiAnalyzer.	string	Maximum length: 127							
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79							
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63							
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default						

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
	Option	Description																
	default	Follow system global setting.																
	SSLv3	SSLv3.																
	TLSv1	TLSv1.																
	TLSv1-1	TLSv1.1.																
	TLSv1-2	TLSv1.2.																
TLSv1-3	TLSv1.3.																	
status	Enable/disable logging to FortiAnalyzer.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.											
	Option	Description																
	enable	Enable logging to FortiAnalyzer.																
disable	Disable logging to FortiAnalyzer.																	
upload-day	Day of week (month) to upload logs.	user	Not Specified															
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.									
	Option	Description																
	daily	Upload log files to FortiAnalyzer once a day.																
	weekly	Upload log files to FortiAnalyzer once a week.																
monthly	Upload log files to FortiAnalyzer once a month.																	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.							
	Option	Description																
	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.																
	realtime	Log directly to FortiAnalyzer in real time.																
	1-minute	Log directly to FortiAnalyzer at least every 1 minute.																
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.																	
upload-time	Time to upload logs (hh:mm).	user	Not Specified															

Parameter	Description	Type	Size	Default
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config log fortianalyzer3 filter

Filters for FortiAnalyzer.

```

config log fortianalyzer3 filter
    Description: Filters for FortiAnalyzer.
    set anomaly [enable|disable]
    set debug [enable|disable]
    set dlp-archive [enable|disable]
    set forti-switch [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set http-transaction [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

config log fortianalyzer3 filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									

Parameter	Description	Type	Size	Default						
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config log fortianalyzer3 override-filter

Override filters for FortiAnalyzer.

```

config log fortianalyzer3 override-filter
  Description: Override filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end

```

config log fortianalyzer3 override-filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
debug	Enable/disable debug logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Debug logging.		
	<i>disable</i>	Disable Debug logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Forti-Switch logging.		
	<i>disable</i>	Disable Forti-Switch logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config log fortianalyzer3 override-setting

Override FortiAnalyzer settings.

```

config log fortianalyzer3 override-setting
  Description: Override FortiAnalyzer settings.
  set access-config [enable|disable]
  set alt-server {string}
  set certificate {string}
  set certificate-verification [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
  set fallback-to-primary [enable|disable]
  set hmac-algorithm {option}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ips-archive [enable|disable]
  set max-log-rate {integer}
  set monitor-failure-retry-period {integer}
  set monitor-keepalive-period {integer}
  set preshared-key {string}
  set priority [default|low]
  set reliable [enable|disable]
  set serial <name1>, <name2>, ...
  set server {string}
  set server-cert-ca {string}
  set source-ip {string}

```

```

set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
set use-management-vdom [enable|disable]
set vrf-select {integer}
end

```

config log fortianalyzer3 override-setting

Parameter	Description	Type	Size	Default
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.		
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.		
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.		
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high
	Option	Description		
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.		
	<i>high</i>	Encrypt logs using high encryption algorithms.		
	<i>low</i>	Encrypt logs using all encryption algorithms.		

Parameter	Description	Type	Size	Default								
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td><i>disable</i></td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.					
Option	Description											
<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.							
Option	Description											
<i>sha256</i>	Use SHA256 as HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.					
Option	Description											
<i>enable</i>	Enable IPS packet archive logging.											
<i>disable</i>	Disable IPS packet archive logging.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5								

Parameter	Description	Type	Size	Default														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63															
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	default	Set FortiAnalyzer log transmission priority to default.	low	Set FortiAnalyzer log transmission priority to low.											
Option	Description																	
default	Set FortiAnalyzer log transmission priority to default.																	
low	Set FortiAnalyzer log transmission priority to low.																	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable reliable logging to FortiAnalyzer.	disable	Disable reliable logging to FortiAnalyzer.											
Option	Description																	
enable	Enable reliable logging to FortiAnalyzer.																	
disable	Disable reliable logging to FortiAnalyzer.																	
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79															
server	The remote FortiAnalyzer.	string	Maximum length: 127															
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	

Parameter	Description	Type	Size	Default										
status	Enable/disable logging to FortiAnalyzer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable logging to FortiAnalyzer.													
<i>disable</i>	Disable logging to FortiAnalyzer.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>daily</i></td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td><i>weekly</i></td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td><i>monthly</i></td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>store-and-upload</i></td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td><i>realtime</i></td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td><i>1-minute</i></td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td><i>5-minute</i></td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.													
<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.													
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0										

config log fortianalyzer3 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer3 setting
  Description: Global FortiAnalyzer settings.
  set access-config [enable|disable]
  set alt-server {string}
  set certificate {string}
  set certificate-verification [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
  set fallback-to-primary [enable|disable]
  set hmac-algorithm {option}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ips-archive [enable|disable]
  set max-log-rate {integer}
  set monitor-failure-retry-period {integer}
  set monitor-keepalive-period {integer}
  set preshared-key {string}
  set priority [default|low]
  set reliable [enable|disable]
  set serial <name1>, <name2>, ...
  set server {string}
  set server-cert-ca {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
  set upload-day {user}
  set upload-interval [daily|weekly|...]
  set upload-option [store-and-upload|realtime|...]
  set upload-time {user}
  set vrf-select {integer}
end
```

config log fortianalyzer3 setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td>disable</td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>				Option	Description	enable	Enable FortiAnalyzer access to configuration and data.	disable	Disable FortiAnalyzer access to configuration and data.
Option	Description									
enable	Enable FortiAnalyzer access to configuration and data.									
disable	Disable FortiAnalyzer access to configuration and data.									

Parameter	Description	Type	Size	Default								
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127									
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35									
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td>disable</td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	enable	Enable identity verification of FortiAnalyzer by use of certificate.	disable	Disable identity verification of FortiAnalyzer by use of certificate.					
Option	Description											
enable	Enable identity verification of FortiAnalyzer by use of certificate.											
disable	Disable identity verification of FortiAnalyzer by use of certificate.											
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high-medium</td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td>high</td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td>low</td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	high-medium	Encrypt logs using high and medium encryption algorithms.	high	Encrypt logs using high encryption algorithms.	low	Encrypt logs using all encryption algorithms.			
Option	Description											
high-medium	Encrypt logs using high and medium encryption algorithms.											
high	Encrypt logs using high encryption algorithms.											
low	Encrypt logs using all encryption algorithms.											
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td>disable</td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	enable	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	disable	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.					
Option	Description											
enable	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
disable	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha256</td><td>Use SHA256 as HMAC algorithm.</td></tr></table>	Option	Description	sha256	Use SHA256 as HMAC algorithm.							
Option	Description											
sha256	Use SHA256 as HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.											
	Option	Description																
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.																
<i>disable</i>	Disable reliable logging to FortiAnalyzer.																	
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79															
server	The remote FortiAnalyzer.	string	Maximum length: 127															
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
ssl-min- proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
	Option	Description																
	<i>default</i>	Follow system global setting.																
	<i>SSLv3</i>	SSLv3.																
	<i>TLSv1</i>	TLSv1.																
	<i>TLSv1-1</i>	TLSv1.1.																
	<i>TLSv1-2</i>	TLSv1.2.																
<i>TLSv1-3</i>	TLSv1.3.																	
status	Enable/disable logging to FortiAnalyzer.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.											
	Option	Description																
	<i>enable</i>	Enable logging to FortiAnalyzer.																
<i>disable</i>	Disable logging to FortiAnalyzer.																	
upload-day	Day of week (month) to upload logs.	user	Not Specified															
upload- interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>daily</i></td><td>Upload log files to FortiAnalyzer once a day.</td></tr></table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
	Option	Description																
<i>daily</i>	Upload log files to FortiAnalyzer once a day.																	

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weekly</i></td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td><i>monthly</i></td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.							
	Option	Description												
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.												
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>store-and-upload</i></td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td><i>realtime</i></td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td><i>1-minute</i></td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td><i>5-minute</i></td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
	Option	Description												
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.												
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.												
	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.												
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0										

config log fortianalyzer-cloud filter

Filters for FortiAnalyzer Cloud.

```

config log fortianalyzer-cloud filter
  Description: Filters for FortiAnalyzer Cloud.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]

```

```

set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log fortianalyzer-cloud filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																		
	<i>dns</i>	DNS detail log.																		
	<i>ssh</i>	SSH log.																		
	<i>ssl</i>	SSL log.																		
	<i>file-filter</i>	File filter log.																		
	<i>icap</i>	ICAP log.																		
	<i>virtual-patch</i>	Virtual patch log.																		
<i>debug</i>	Debug log.																			
filter	Free style filter string.	string	Maximum length: 1023																	
filter-type	Include/exclude logs that match the filter.	option	-	include																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.													
	Option	Description																		
	<i>include</i>	Include logs that match the filter.																		
<i>exclude</i>	Exclude logs that match the filter.																			
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295																	

config log fortianalyzer-cloud override-filter

Override filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud override-filter
  Description: Override filters for FortiAnalyzer Cloud.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
```

```

set gtp [enable|disable]
set http-transaction [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log fortianalyzer-cloud override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									

Parameter	Description	Type	Size	Default																		
gtp *	Enable/disable GTP messages logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable GTP messages logging.</td></tr><tr><td>disable</td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	enable	Enable GTP messages logging.	disable	Disable GTP messages logging.															
Option	Description																					
enable	Enable GTP messages logging.																					
disable	Disable GTP messages logging.																					
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable http transaction logging.</td></tr><tr><td>disable</td><td>Disable http transaction logging.</td></tr></table>	Option	Description	enable	Enable http transaction logging.	disable	Disable http transaction logging.															
Option	Description																					
enable	Enable http transaction logging.																					
disable	Disable http transaction logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable local in or out traffic logging.</td></tr><tr><td>disable</td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	enable	Enable local in or out traffic logging.	disable	Disable local in or out traffic logging.															
Option	Description																					
enable	Enable local in or out traffic logging.																					
disable	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable multicast traffic logging.</td></tr><tr><td>disable</td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	enable	Enable multicast traffic logging.	disable	Disable multicast traffic logging.															
Option	Description																					
enable	Enable multicast traffic logging.																					
disable	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>emergency</td><td>Emergency level.</td></tr><tr><td>alert</td><td>Alert level.</td></tr><tr><td>critical</td><td>Critical level.</td></tr><tr><td>error</td><td>Error level.</td></tr><tr><td>warning</td><td>Warning level.</td></tr><tr><td>notification</td><td>Notification level.</td></tr><tr><td>information</td><td>Information level.</td></tr><tr><td>debug</td><td>Debug level.</td></tr></table>	Option	Description	emergency	Emergency level.	alert	Alert level.	critical	Critical level.	error	Error level.	warning	Warning level.	notification	Notification level.	information	Information level.	debug	Debug level.			
Option	Description																					
emergency	Emergency level.																					
alert	Alert level.																					
critical	Critical level.																					
error	Error level.																					
warning	Warning level.																					
notification	Notification level.																					
information	Information level.																					
debug	Debug level.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																		
	<i>dns</i>	DNS detail log.																		
	<i>ssh</i>	SSH log.																		
	<i>ssl</i>	SSL log.																		
	<i>file-filter</i>	File filter log.																		
	<i>icap</i>	ICAP log.																		
	<i>virtual-patch</i>	Virtual patch log.																		
<i>debug</i>	Debug log.																			
filter	Free style filter string.	string	Maximum length: 1023																	
filter-type	Include/exclude logs that match the filter.	option	-	include																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.													
	Option	Description																		
	<i>include</i>	Include logs that match the filter.																		
<i>exclude</i>	Exclude logs that match the filter.																			
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																	

config log fortianalyzer-cloud override-setting

Override FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud override-setting
    Description: Override FortiAnalyzer Cloud settings.
    set status [enable|disable]
end
```

config log fortianalyzer-cloud override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		

config log fortianalyzer-cloud setting

Global FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud setting
    Description: Global FortiAnalyzer Cloud settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm {option}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set preshared-key {string}
    set priority [default|low]
    set serial <name1>, <name2>, ...
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
    set vrf-select {integer}
end
```

config log fortianalyzer-cloud setting

Parameter	Description	Type	Size	Default
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.		
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.		
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.		
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high
	Option	Description		
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.		
	<i>high</i>	Encrypt logs using high encryption algorithms.		
	<i>low</i>	Encrypt logs using all encryption algorithms.		
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
	Option	Description																
	default	Follow system global setting.																
	SSLv3	SSLv3.																
	TLSv1	TLSv1.																
	TLSv1-1	TLSv1.1.																
	TLSv1-2	TLSv1.2.																
TLSv1-3	TLSv1.3.																	
status	Enable/disable logging to FortiAnalyzer.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.											
	Option	Description																
	enable	Enable logging to FortiAnalyzer.																
disable	Disable logging to FortiAnalyzer.																	
upload-day	Day of week (month) to upload logs.	user	Not Specified															
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.									
	Option	Description																
	daily	Upload log files to FortiAnalyzer once a day.																
	weekly	Upload log files to FortiAnalyzer once a week.																
monthly	Upload log files to FortiAnalyzer once a month.																	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.							
	Option	Description																
	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.																
	realtime	Log directly to FortiAnalyzer in real time.																
	1-minute	Log directly to FortiAnalyzer at least every 1 minute.																
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.																	
upload-time	Time to upload logs (hh:mm).	user	Not Specified															

Parameter	Description	Type	Size	Default
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config log fortiguard filter

Filters for FortiCloud.

```

config log fortiguard filter
    Description: Filters for FortiCloud.
    set anomaly [enable|disable]
    set debug [enable|disable]
    set forti-switch [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set http-transaction [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

config log fortiguard filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
debug	Enable/disable debug logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Debug logging.		
	<i>disable</i>	Disable Debug logging.		
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Forti-Switch logging.		
	<i>disable</i>	Disable Forti-Switch logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default																																						
category	Log category.	option	-	traffic																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr><tr><td>virtual-patch</td><td>Virtual patch log.</td></tr><tr><td>debug</td><td>Debug log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.	virtual-patch	Virtual patch log.	debug	Debug log.			
	Option	Description																																								
	traffic	Traffic log.																																								
	event	Event log.																																								
	virus	Antivirus log.																																								
	webfilter	Web filter log.																																								
	attack	Attack log.																																								
	spam	Antispam log.																																								
	anomaly	Anomaly log.																																								
	voip	VoIP log.																																								
	dlp	DLP log.																																								
	app-ctrl	Application control log.																																								
	waf	Web application firewall log.																																								
	dns	DNS detail log.																																								
	ssh	SSH log.																																								
	ssl	SSL log.																																								
	file-filter	File filter log.																																								
	icap	ICAP log.																																								
	virtual-patch	Virtual patch log.																																								
	debug	Debug log.																																								
filter	Free style filter string.	string	Maximum length: 1023																																							
filter-type	Include/exclude logs that match the filter.	option	-	include																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																																			
	Option	Description																																								
	include	Include logs that match the filter.																																								
exclude	Exclude logs that match the filter.																																									
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																																							

config log fortiguard override-filter

Override filters for FortiCloud.

```
config log fortiguard override-filter
  Description: Override filters for FortiCloud.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end
```

config log fortiguard override-filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
debug	Enable/disable debug logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Debug logging.		
	<i>disable</i>	Disable Debug logging.		
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Forti-Switch logging.		
	<i>disable</i>	Disable Forti-Switch logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																																						
	<i>event</i>	Event log.																																						
	<i>virus</i>	Antivirus log.																																						
	<i>webfilter</i>	Web filter log.																																						
	<i>attack</i>	Attack log.																																						
	<i>spam</i>	Antispam log.																																						
	<i>anomaly</i>	Anomaly log.																																						
	<i>voip</i>	VoIP log.																																						
	<i>dlp</i>	DLP log.																																						
	<i>app-ctrl</i>	Application control log.																																						
	<i>waf</i>	Web application firewall log.																																						
	<i>dns</i>	DNS detail log.																																						
	<i>ssh</i>	SSH log.																																						
	<i>ssl</i>	SSL log.																																						
	<i>file-filter</i>	File filter log.																																						
	<i>icap</i>	ICAP log.																																						
	<i>virtual-patch</i>	Virtual patch log.																																						
<i>debug</i>	Debug log.																																							
filter	Free style filter string.	string	Maximum length: 1023																																					
filter-type	Include/exclude logs that match the filter.	option	-	include																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																																	
	Option	Description																																						
	<i>include</i>	Include logs that match the filter.																																						
<i>exclude</i>	Exclude logs that match the filter.																																							
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295																																					

config log fortiguard override-setting

Override global FortiCloud logging settings for this VDOM.

```

config log fortiguard override-setting
    Description: Override global FortiCloud logging settings for this VDOM.
    set access-config [enable|disable]
    set max-log-rate {integer}
    set override [enable|disable]
    set priority [default|low]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
end

```

config log fortiguard override-setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiCloud access to configuration and data.</td></tr><tr><td>disable</td><td>Disable FortiCloud access to configuration and data.</td></tr></table>	Option	Description	enable	Enable FortiCloud access to configuration and data.	disable	Disable FortiCloud access to configuration and data.			
Option	Description									
enable	Enable FortiCloud access to configuration and data.									
disable	Disable FortiCloud access to configuration and data.									
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
override	Overriding FortiCloud settings for this VDOM or use global settings.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override FortiCloud logging settings.</td></tr><tr><td>disable</td><td>Use global FortiCloud logging settings.</td></tr></table>	Option	Description	enable	Override FortiCloud logging settings.	disable	Use global FortiCloud logging settings.			
Option	Description									
enable	Override FortiCloud logging settings.									
disable	Use global FortiCloud logging settings.									
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiCloud log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiCloud log transmission priority to low.</td></tr></table>	Option	Description	default	Set FortiCloud log transmission priority to default.	low	Set FortiCloud log transmission priority to low.			
Option	Description									
default	Set FortiCloud log transmission priority to default.									
low	Set FortiCloud log transmission priority to low.									
status	Enable/disable logging to FortiCloud.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable logging to FortiCloud.		
	<i>disable</i>	Disable logging to FortiCloud.		
upload-day	Day of week to roll logs.	user	Not Specified	
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily
	Option	Description		
	<i>daily</i>	Upload log files to FortiCloud once a day.		
	<i>weekly</i>	Upload log files to FortiCloud once a week.		
	<i>monthly</i>	Upload log files to FortiCloud once a month.		
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute
	Option	Description		
	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.		
	<i>realtime</i>	Log directly to FortiCloud in real time.		
	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.		
	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.		
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified	

config log fortiguard setting

Configure logging to FortiCloud.

```
config log fortiguard setting
  Description: Configure logging to FortiCloud.
  set access-config [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set max-log-rate {integer}
  set priority [default|low]
  set source-ip {ipv4-address}
```

```

set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
set vrf-select {integer}
end

```

config log fortiguard setting

Parameter	Description	Type	Size	Default								
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiCloud access to configuration and data.</td></tr><tr><td>disable</td><td>Disable FortiCloud access to configuration and data.</td></tr></table>	Option	Description	enable	Enable FortiCloud access to configuration and data.	disable	Disable FortiCloud access to configuration and data.					
Option	Description											
enable	Enable FortiCloud access to configuration and data.											
disable	Disable FortiCloud access to configuration and data.											
conn-timeout	FortiGate Cloud connection timeout in seconds.	integer	Minimum value: 1 Maximum value: 3600	10								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiCloud.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high-medium</td><td>Encrypt logs using high and medium encryption.</td></tr><tr><td>high</td><td>Encrypt logs using high encryption.</td></tr><tr><td>low</td><td>Encrypt logs using low encryption.</td></tr></table>	Option	Description	high-medium	Encrypt logs using high and medium encryption.	high	Encrypt logs using high encryption.	low	Encrypt logs using low encryption.			
Option	Description											
high-medium	Encrypt logs using high and medium encryption.											
high	Encrypt logs using high encryption.											
low	Encrypt logs using low encryption.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											

Parameter	Description	Type	Size	Default														
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiCloud log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiCloud log transmission priority to low.</td></tr></table>	Option	Description	default	Set FortiCloud log transmission priority to default.	low	Set FortiCloud log transmission priority to low.											
Option	Description																	
default	Set FortiCloud log transmission priority to default.																	
low	Set FortiCloud log transmission priority to low.																	
source-ip	Source IP address used to connect FortiCloud.	ipv4-address	Not Specified	0.0.0.0														
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
status	Enable/disable logging to FortiCloud.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiCloud.</td></tr><tr><td>disable</td><td>Disable logging to FortiCloud.</td></tr></table>	Option	Description	enable	Enable logging to FortiCloud.	disable	Disable logging to FortiCloud.											
Option	Description																	
enable	Enable logging to FortiCloud.																	
disable	Disable logging to FortiCloud.																	
upload-day	Day of week to roll logs.	user	Not Specified															
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiCloud once a day.</td></tr></table>	Option	Description	daily	Upload log files to FortiCloud once a day.													
Option	Description																	
daily	Upload log files to FortiCloud once a day.																	

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weekly</i></td><td>Upload log files to FortiCloud once a week.</td></tr><tr><td><i>monthly</i></td><td>Upload log files to FortiCloud once a month.</td></tr></table>	Option	Description	<i>weekly</i>	Upload log files to FortiCloud once a week.	<i>monthly</i>	Upload log files to FortiCloud once a month.							
	Option	Description												
	<i>weekly</i>	Upload log files to FortiCloud once a week.												
<i>monthly</i>	Upload log files to FortiCloud once a month.													
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>store-and-upload</i></td><td>Log to the hard disk and then upload logs to FortiCloud.</td></tr><tr><td><i>realtime</i></td><td>Log directly to FortiCloud in real time.</td></tr><tr><td><i>1-minute</i></td><td>Log directly to FortiCloud at 1-minute intervals.</td></tr><tr><td><i>5-minute</i></td><td>Log directly to FortiCloud at 5-minute intervals.</td></tr></table>	Option	Description	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.	<i>realtime</i>	Log directly to FortiCloud in real time.	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.			
	Option	Description												
	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.												
	<i>realtime</i>	Log directly to FortiCloud in real time.												
	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.												
<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.													
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified											
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0										

config log gui-display

Configure how log messages are displayed on the GUI.

```
config log gui-display
    Description: Configure how log messages are displayed on the GUI.
    set fortiview-unscanned-apps [enable|disable]
    set resolve-apps [enable|disable]
    set resolve-hosts [enable|disable]
end
```

config log gui-display

Parameter	Description	Type	Size	Default
fortiview-unscanned-apps	Enable/disable showing unscanned traffic in FortiView application charts.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable showing unscanned traffic.		
	<i>disable</i>	Disable showing unscanned traffic.		
resolve-apps	Resolve unknown applications on the GUI using Fortinet's remote application database.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable unknown applications on the GUI.		
	<i>disable</i>	Disable unknown applications on the GUI.		
resolve-hosts	Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable resolving IP addresses to hostnames.		
	<i>disable</i>	Disable resolving IP addresses to hostnames.		

config log memory filter

Filters for memory buffer.

```

config log memory filter
  Description: Filters for memory buffer.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]

```

```
set ztna-traffic [enable|disable]
end
```

config log memory filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.					
Option	Description									
<i>enable</i>	Enable http transaction logging.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable **
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Log every message above and including this severity level.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

** Values may differ between models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config log memory global-setting

Global settings for memory logging.

```

config log memory global-setting
    Description: Global settings for memory logging.
    set full-final-warning-threshold {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set max-size {integer}
end

```

config log memory global-setting

Parameter	Description	Type	Size	Default
full-final-warning-threshold	Log full final warning threshold as a percent (3 - 100, default = 95).	integer	Minimum value: 3 Maximum value: 100	95
full-first-warning-threshold	Log full first warning threshold as a percent (1 - 98, default = 75).	integer	Minimum value: 1 Maximum value: 98	75

Parameter	Description	Type	Size	Default
full-second-warning-threshold	Log full second warning threshold as a percent (2 - 99, default = 90).	integer	Minimum value: 2 Maximum value: 99	90
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 4294967295	168438988 **

** Values may differ between models.

config log memory setting

Settings for memory buffer.

```
config log memory setting
    Description: Settings for memory buffer.
    set status [enable|disable]
end
```

config log memory setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to the FortiGate's memory.	option	-	enable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging to memory.</td></tr><tr><td><i>disable</i></td><td>Disable logging to memory.</td></tr></table>				Option	Description	<i>enable</i>	Enable logging to memory.	<i>disable</i>	Disable logging to memory.
	Option	Description								
	<i>enable</i>	Enable logging to memory.								
<i>disable</i>	Disable logging to memory.									

** Values may differ between models.

config log null-device filter

Filters for null device logging.

```
config log null-device filter
    Description: Filters for null device logging.
    set anomaly [enable|disable]
    set debug [enable|disable]
    set forti-switch [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
```

```

Description: Free style filters.
edit <id>
    set category [traffic|event|...]
    set filter {string}
    set filter-type [include|exclude]
next
end
set gtp [enable|disable]
set http-transaction [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log null-device filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable anomaly logging.</td></tr><tr><td>disable</td><td>Disable anomaly logging.</td></tr></table>	Option	Description	enable	Enable anomaly logging.	disable	Disable anomaly logging.			
Option	Description									
enable	Enable anomaly logging.									
disable	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Debug logging.</td></tr><tr><td>disable</td><td>Disable Debug logging.</td></tr></table>	Option	Description	enable	Enable Debug logging.	disable	Disable Debug logging.			
Option	Description									
enable	Enable Debug logging.									
disable	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Forti-Switch logging.</td></tr><tr><td>disable</td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	enable	Enable Forti-Switch logging.	disable	Disable Forti-Switch logging.			
Option	Description									
enable	Enable Forti-Switch logging.									
disable	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable forward traffic logging.</td></tr><tr><td>disable</td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	enable	Enable forward traffic logging.	disable	Disable forward traffic logging.			
Option	Description									
enable	Enable forward traffic logging.									
disable	Disable forward traffic logging.									

Parameter	Description	Type	Size	Default																		
gtp *	Enable/disable GTP messages logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.															
Option	Description																					
<i>enable</i>	Enable GTP messages logging.																					
<i>disable</i>	Disable GTP messages logging.																					
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.															
Option	Description																					
<i>enable</i>	Enable http transaction logging.																					
<i>disable</i>	Disable http transaction logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																		
	<i>dns</i>	DNS detail log.																		
	<i>ssh</i>	SSH log.																		
	<i>ssl</i>	SSL log.																		
	<i>file-filter</i>	File filter log.																		
	<i>icap</i>	ICAP log.																		
	<i>virtual-patch</i>	Virtual patch log.																		
<i>debug</i>	Debug log.																			
filter	Free style filter string.	string	Maximum length: 1023																	
filter-type	Include/exclude logs that match the filter.	option	-	include																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.													
	Option	Description																		
	<i>include</i>	Include logs that match the filter.																		
<i>exclude</i>	Exclude logs that match the filter.																			
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																	

config log null-device setting

Settings for null device logging.

```
config log null-device setting
    Description: Settings for null device logging.
    set status [enable|disable]
end
```

config log null-device setting

Parameter	Description	Type	Size	Default
status	Enable/disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).		
	<i>disable</i>	Disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).		

config log setting

Configure general log settings.

```
config log setting
    Description: Configure general log settings.
    set anonymization-hash {string}
    set brief-traffic-format [enable|disable]
    set custom-log-fields <field-id1>, <field-id2>, ...
    set daemon-log [enable|disable]
    set expolicy-implicit-log [enable|disable]
    set extended-log [enable|disable]
    set extended-utm-log [enable|disable]
    set faz-override [enable|disable]
    set fortiview-weekly-data [enable|disable]
    set fwpolicy-implicit-log [enable|disable]
    set fwpolicy6-implicit-log [enable|disable]
    set local-in-allow [enable|disable]
    set local-in-deny-broadcast [enable|disable]
    set local-in-deny-unicast [enable|disable]
    set local-in-policy-log [enable|disable]
    set local-out [enable|disable]
    set local-out-ioc-detection [enable|disable]
    set log-policy-comment [enable|disable]
    set log-user-in-upper [enable|disable]
    set long-live-session-stat [enable|disable]
    set neighbor-event [enable|disable]
    set resolve-ip [enable|disable]
    set resolve-port [enable|disable]
    set rest-api-get [enable|disable]
    set rest-api-set [enable|disable]
    set syslog-override [enable|disable]
    set user-anonymize [enable|disable]
end
```

config log setting

Parameter	Description	Type	Size	Default						
anonymization-hash	User name anonymization hash salt.	string	Maximum length: 32							
brief-traffic-format	Enable/disable brief format traffic logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable brief format traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable brief format traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable brief format traffic logging.	<i>disable</i>	Disable brief format traffic logging.			
Option	Description									
<i>enable</i>	Enable brief format traffic logging.									
<i>disable</i>	Disable brief format traffic logging.									
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35							
daemon-log	Enable/disable daemon logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable daemon logging.</td></tr><tr><td><i>disable</i></td><td>Disable daemon logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable daemon logging.	<i>disable</i>	Disable daemon logging.			
Option	Description									
<i>enable</i>	Enable daemon logging.									
<i>disable</i>	Disable daemon logging.									
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable explicit proxy firewall implicit policy logging.</td></tr><tr><td><i>disable</i></td><td>Disable explicit proxy firewall implicit policy logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable explicit proxy firewall implicit policy logging.	<i>disable</i>	Disable explicit proxy firewall implicit policy logging.			
Option	Description									
<i>enable</i>	Enable explicit proxy firewall implicit policy logging.									
<i>disable</i>	Disable explicit proxy firewall implicit policy logging.									
extended-log	Enable/disable extended traffic logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable extended traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable extended traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable extended traffic logging.	<i>disable</i>	Disable extended traffic logging.			
Option	Description									
<i>enable</i>	Enable extended traffic logging.									
<i>disable</i>	Disable extended traffic logging.									
extended-utm-log	Enable/disable extended UTM logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable extended UTM logging.</td></tr><tr><td><i>disable</i></td><td>Disable extended UTM logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable extended UTM logging.	<i>disable</i>	Disable extended UTM logging.			
Option	Description									
<i>enable</i>	Enable extended UTM logging.									
<i>disable</i>	Disable extended UTM logging.									
faz-override	Enable/disable override FortiAnalyzer settings.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable override FortiAnalyzer settings.		
	<i>disable</i>	Disable override FortiAnalyzer settings.		
fortiview-weekly-data *	Enable/disable FortiView weekly data.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiView weekly data.		
	<i>disable</i>	Disable FortiView weekly data.		
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable implicit firewall policy logging.		
	<i>disable</i>	Disable implicit firewall policy logging.		
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable implicit firewall policy6 logging.		
	<i>disable</i>	Disable implicit firewall policy6 logging.		
local-in-allow	Enable/disable local-in-allow logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable local-in-allow logging.		
	<i>disable</i>	Disable local-in-allow logging.		
local-in-deny-broadcast	Enable/disable local-in-deny-broadcast logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable local-in-deny-broadcast logging.		
	<i>disable</i>	Disable local-in-deny-broadcast logging.		
local-in-deny-unicast	Enable/disable local-in-deny-unicast logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local-in-deny-unicast logging.		
	<i>disable</i>	Disable local-in-deny-unicast logging.		
local-in-policy-log	Enable/disable local-in-policy logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable local-in-policy logging.		
	<i>disable</i>	Disable local-in-policy logging.		
local-out	Enable/disable local-out logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local-out logging.		
	<i>disable</i>	Disable local-out logging.		
local-out-ioc-detection	Enable/disable local-out traffic IoC detection. Requires local-out to be enabled.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local-out traffic IoC detection. Requires local-out to be enabled.		
	<i>disable</i>	Disable local-out traffic IoC detection.		
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable inserting policy comments into traffic logs.		
	<i>disable</i>	Disable inserting policy comments into traffic logs.		
log-user-in-upper	Enable/disable logs with user-in-upper.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logs with user-in-upper.		
	<i>disable</i>	Disable logs with user-in-upper.		
long-live-session-stat	Enable/disable long-live-session statistics logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable long-live-session statistics logging.		
	<i>disable</i>	Disable long-live-session statistics logging.		
neighbor-event	Enable/disable neighbor event logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable neighbor event logging.		
	<i>disable</i>	Disable neighbor event logging.		
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable adding resolved domain names to traffic logs.		
	<i>disable</i>	Disable adding resolved domain names to traffic logs.		
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable adding resolved service names to traffic logs.		
	<i>disable</i>	Disable adding resolved service names to traffic logs.		
rest-api-get	Enable/disable REST API GET request logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable GET REST API logging.		
	<i>disable</i>	Disable GET REST API logging.		
rest-api-set	Enable/disable REST API POST/PUT/DELETE request logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable POST/PUT/DELETE REST API logging.		
	<i>disable</i>	Disable POST/PUT/DELETE REST API logging.		
syslog-override	Enable/disable override Syslog settings.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable override Syslog settings.		
	<i>disable</i>	Disable override Syslog settings.		
user-anonymize	Enable/disable anonymizing user names in log messages.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable anonymizing user names in log messages.		
	<i>disable</i>	Disable anonymizing user names in log messages.		

* This parameter may not exist in some models.

config log syslogd filter

Filters for remote system server.

```

config log syslogd filter
    Description: Filters for remote system server.
    set anomaly [enable|disable]
    set debug [enable|disable]
    set forti-switch [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set http-transaction [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

config log syslogd filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config log syslogd override-filter

Override filters for remote system server.

```

config log syslogd override-filter
  Description: Override filters for remote system server.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end

```

config log syslogd override-filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
debug	Enable/disable debug logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Debug logging.		
	<i>disable</i>	Disable Debug logging.		
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Forti-Switch logging.		
	<i>disable</i>	Disable Forti-Switch logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config log syslogd override-setting

Override settings for remote syslog server.

```

config log syslogd override-setting
  Description: Override settings for remote syslog server.
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set custom {string}
      set name {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set max-log-rate {integer}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set priority [default|low]
  set server {string}
  set source-ip {string}
  set source-ip-interface {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
  set use-management-vdom [enable|disable]
  set vrf-select {integer}
end

```

config log syslogd override-setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option	Description		
	high-medium	SSL communication with high and medium encryption algorithms.		
	high	SSL communication with high encryption algorithms.		
	low	SSL communication with low encryption algorithms.		
	disable	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	Option	Description		
	kernel	Kernel messages.		
	user	Random user-level messages.		
	mail	Mail system.		
	daemon	System daemons.		
	auth	Security/authorization messages.		
	syslog	Messages generated internally by syslog.		
	lpr	Line printer subsystem.		
	news	Network news subsystem.		
	uucp	Network news subsystem.		
	cron	Clock daemon.		
	authpriv	Security/authorization messages (private).		
	ftp	FTP daemon.		
	ntp	NTP daemon.		
	audit	Log audit.		
	alert	Log alert.		
	clock	Clock daemon.		
	local0	Reserved for local use.		
local1	Reserved for local use.			

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																
	<i>local2</i>	Reserved for local use.																
	<i>local3</i>	Reserved for local use.																
	<i>local4</i>	Reserved for local use.																
	<i>local5</i>	Reserved for local use.																
	<i>local6</i>	Reserved for local use.																
<i>local7</i>	Reserved for local use.																	
format	Log format.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.					
	Option	Description																
	<i>default</i>	Syslog format.																
	<i>csv</i>	CSV (Comma Separated Values) format.																
	<i>cef</i>	CEF (Common Event Format) format.																
	<i>rfc5424</i>	Syslog RFC5424 format.																
<i>json</i>	JSON (JavaScript Object Notation) format.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.									
	Option	Description																
	<i>auto</i>	Set outgoing interface automatically.																
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																
<i>specify</i>	Set outgoing interface manually.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.													
	Option	Description																
<i>udp</i>	Enable syslogging over UDP.																	

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
	Option	Description																
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																	
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514														
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set Syslog transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.											
	Option	Description																
	<i>default</i>	Set Syslog transmission priority to default.																
<i>low</i>	Set Syslog transmission priority to low.																	
server	Address of remote syslog server.	string	Maximum length: 127															
source-ip	Source IP address of syslog.	string	Maximum length: 63															
source-ip-interface	Source interface of syslog.	string	Maximum length: 15															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
	Option	Description																
	<i>default</i>	Follow system global setting.																
	<i>SSLv3</i>	SSLv3.																
	<i>TLSv1</i>	TLSv1.																
	<i>TLSv1-1</i>	TLSv1.1.																
	<i>TLSv1-2</i>	TLSv1.2.																
<i>TLSv1-3</i>	TLSv1.3.																	
status	Enable/disable remote syslog logging.	option	-	disable														

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.			
	Option	Description								
	<i>enable</i>	Log to remote syslog server.								
<i>disable</i>	Do not log to remote syslog server.									
use-management-vdom	Enable/disable use of management VDOM as source VDOM for logs sent to syslog server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of management VDOM as source VDOM.</td></tr><tr><td><i>disable</i></td><td>Use the current VDOM as source VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of management VDOM as source VDOM.	<i>disable</i>	Use the current VDOM as source VDOM.			
	Option	Description								
	<i>enable</i>	Enable use of management VDOM as source VDOM.								
<i>disable</i>	Use the current VDOM as source VDOM.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log syslogd setting

Global settings for remote syslog server.

```

config log syslogd setting
  Description: Global settings for remote syslog server.
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set custom {string}
      set name {string}
    next

```



```

end
set enc-algorithm [high-medium|high|...]
set facility [kernel|user|...]
set format [default|csv|...]
set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|legacy-reliable|...]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set source-ip-interface {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set vrf-select {integer}
end

```

config log syslogd setting

Parameter	Description	Type	Size	Default														
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high-medium</td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td>high</td><td>SSL communication with high encryption algorithms.</td></tr><tr><td>low</td><td>SSL communication with low encryption algorithms.</td></tr><tr><td>disable</td><td>Disable SSL communication.</td></tr></table>	Option	Description	high-medium	SSL communication with high and medium encryption algorithms.	high	SSL communication with high encryption algorithms.	low	SSL communication with low encryption algorithms.	disable	Disable SSL communication.							
Option	Description																	
high-medium	SSL communication with high and medium encryption algorithms.																	
high	SSL communication with high encryption algorithms.																	
low	SSL communication with low encryption algorithms.																	
disable	Disable SSL communication.																	
facility	Remote syslog facility.	option	-	local7														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>kernel</td><td>Kernel messages.</td></tr><tr><td>user</td><td>Random user-level messages.</td></tr><tr><td>mail</td><td>Mail system.</td></tr><tr><td>daemon</td><td>System daemons.</td></tr><tr><td>auth</td><td>Security/authorization messages.</td></tr><tr><td>syslog</td><td>Messages generated internally by syslog.</td></tr></table>	Option	Description	kernel	Kernel messages.	user	Random user-level messages.	mail	Mail system.	daemon	System daemons.	auth	Security/authorization messages.	syslog	Messages generated internally by syslog.			
Option	Description																	
kernel	Kernel messages.																	
user	Random user-level messages.																	
mail	Mail system.																	
daemon	System daemons.																	
auth	Security/authorization messages.																	
syslog	Messages generated internally by syslog.																	

Parameter	Description	Type	Size	Default																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																								
	<i>lpr</i>	Line printer subsystem.																																								
	<i>news</i>	Network news subsystem.																																								
	<i>uucp</i>	Network news subsystem.																																								
	<i>cron</i>	Clock daemon.																																								
	<i>authpriv</i>	Security/authorization messages (private).																																								
	<i>ftp</i>	FTP daemon.																																								
	<i>ntp</i>	NTP daemon.																																								
	<i>audit</i>	Log audit.																																								
	<i>alert</i>	Log alert.																																								
	<i>clock</i>	Clock daemon.																																								
	<i>local0</i>	Reserved for local use.																																								
	<i>local1</i>	Reserved for local use.																																								
	<i>local2</i>	Reserved for local use.																																								
	<i>local3</i>	Reserved for local use.																																								
	<i>local4</i>	Reserved for local use.																																								
	<i>local5</i>	Reserved for local use.																																								
	<i>local6</i>	Reserved for local use.																																								
	<i>local7</i>	Reserved for local use.																																								
format	Log format.	option	-	default																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.																													
	Option	Description																																								
	<i>default</i>	Syslog format.																																								
	<i>csv</i>	CSV (Comma Separated Values) format.																																								
	<i>cef</i>	CEF (Common Event Format) format.																																								
	<i>rfc5424</i>	Syslog RFC5424 format.																																								
<i>json</i>	JSON (JavaScript Object Notation) format.																																									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																																							

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option	Description		
	<i>udp</i>	Enable syslogging over UDP.		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		
server	Address of remote syslog server.	string	Maximum length: 127	
source-ip	Source IP address of syslog.	string	Maximum length: 63	
source-ip-interface	Source interface of syslog.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default														
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
	Option	Description																
	default	Follow system global setting.																
	SSLv3	SSLv3.																
	TLSv1	TLSv1.																
	TLSv1-1	TLSv1.1.																
	TLSv1-2	TLSv1.2.																
TLSv1-3	TLSv1.3.																	
status	Enable/disable remote syslog logging.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Log to remote syslog server.</td></tr><tr><td>disable</td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	enable	Log to remote syslog server.	disable	Do not log to remote syslog server.											
	Option	Description																
	enable	Log to remote syslog server.																
disable	Do not log to remote syslog server.																	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0														

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log syslogd2 filter

Filters for remote system server.

```

config log syslogd2 filter
    Description: Filters for remote system server.
    set anomaly [enable|disable]
    set debug [enable|disable]
    set forti-switch [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set http-transaction [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

config log syslogd2 filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									

Parameter	Description	Type	Size	Default								
forward-traffic	Enable/disable forward traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable forward traffic logging.</td></tr><tr><td>disable</td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	enable	Enable forward traffic logging.	disable	Disable forward traffic logging.					
Option	Description											
enable	Enable forward traffic logging.											
disable	Disable forward traffic logging.											
gtp *	Enable/disable GTP messages logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable GTP messages logging.</td></tr><tr><td>disable</td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	enable	Enable GTP messages logging.	disable	Disable GTP messages logging.					
Option	Description											
enable	Enable GTP messages logging.											
disable	Disable GTP messages logging.											
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable http transaction logging.</td></tr><tr><td>disable</td><td>Disable http transaction logging.</td></tr></table>	Option	Description	enable	Enable http transaction logging.	disable	Disable http transaction logging.					
Option	Description											
enable	Enable http transaction logging.											
disable	Disable http transaction logging.											
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable local in or out traffic logging.</td></tr><tr><td>disable</td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	enable	Enable local in or out traffic logging.	disable	Disable local in or out traffic logging.					
Option	Description											
enable	Enable local in or out traffic logging.											
disable	Disable local in or out traffic logging.											
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable multicast traffic logging.</td></tr><tr><td>disable</td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	enable	Enable multicast traffic logging.	disable	Disable multicast traffic logging.					
Option	Description											
enable	Enable multicast traffic logging.											
disable	Disable multicast traffic logging.											
severity	Lowest severity level to log.	option	-	information								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>emergency</td><td>Emergency level.</td></tr><tr><td>alert</td><td>Alert level.</td></tr><tr><td>critical</td><td>Critical level.</td></tr></table>	Option	Description	emergency	Emergency level.	alert	Alert level.	critical	Critical level.			
Option	Description											
emergency	Emergency level.											
alert	Alert level.											
critical	Critical level.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																																
	<i>attack</i>	Attack log.																																
	<i>spam</i>	Antispam log.																																
	<i>anomaly</i>	Anomaly log.																																
	<i>voip</i>	VoIP log.																																
	<i>dlp</i>	DLP log.																																
	<i>app-ctrl</i>	Application control log.																																
	<i>waf</i>	Web application firewall log.																																
	<i>dns</i>	DNS detail log.																																
	<i>ssh</i>	SSH log.																																
	<i>ssl</i>	SSL log.																																
	<i>file-filter</i>	File filter log.																																
	<i>icap</i>	ICAP log.																																
	<i>virtual-patch</i>	Virtual patch log.																																
<i>debug</i>	Debug log.																																	
filter	Free style filter string.	string	Maximum length: 1023																															
filter-type	Include/exclude logs that match the filter.	option	-	include																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																											
	Option	Description																																
	<i>include</i>	Include logs that match the filter.																																
<i>exclude</i>	Exclude logs that match the filter.																																	
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																															

config log syslogd2 override-filter

Override filters for remote system server.

```
config log syslogd2 override-filter
  Description: Override filters for remote system server.
  set anomaly [enable|disable]
  set debug [enable|disable]
```



```

set forti-switch [enable|disable]
set forward-traffic [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set http-transaction [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log syslogd2 override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																												
	<i>anomaly</i>	Anomaly log.																												
	<i>voip</i>	VoIP log.																												
	<i>dlp</i>	DLP log.																												
	<i>app-ctrl</i>	Application control log.																												
	<i>waf</i>	Web application firewall log.																												
	<i>dns</i>	DNS detail log.																												
	<i>ssh</i>	SSH log.																												
	<i>ssl</i>	SSL log.																												
	<i>file-filter</i>	File filter log.																												
	<i>icap</i>	ICAP log.																												
	<i>virtual-patch</i>	Virtual patch log.																												
<i>debug</i>	Debug log.																													
filter	Free style filter string.	string	Maximum length: 1023																											
filter-type	Include/exclude logs that match the filter.	option	-	include																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																							
	Option	Description																												
	<i>include</i>	Include logs that match the filter.																												
<i>exclude</i>	Exclude logs that match the filter.																													
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																											

config log syslogd2 override-setting

Override settings for remote syslog server.

```

config log syslogd2 override-setting
    Description: Override settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}

```

```

        set name {string}
    next
end
set enc-algorithm [high-medium|high|...]
set facility [kernel|user|...]
set format [default|csv|...]
set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|legacy-reliable|...]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set source-ip-interface {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set use-management-vdom [enable|disable]
set vrf-select {integer}
end

```

config log syslogd2 override-setting

Parameter	Description	Type	Size	Default										
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35											
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high-medium</td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td>high</td><td>SSL communication with high encryption algorithms.</td></tr><tr><td>low</td><td>SSL communication with low encryption algorithms.</td></tr><tr><td>disable</td><td>Disable SSL communication.</td></tr></table>	Option	Description	high-medium	SSL communication with high and medium encryption algorithms.	high	SSL communication with high encryption algorithms.	low	SSL communication with low encryption algorithms.	disable	Disable SSL communication.			
Option	Description													
high-medium	SSL communication with high and medium encryption algorithms.													
high	SSL communication with high encryption algorithms.													
low	SSL communication with low encryption algorithms.													
disable	Disable SSL communication.													
facility	Remote syslog facility.	option	-	local7										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>kernel</td><td>Kernel messages.</td></tr><tr><td>user</td><td>Random user-level messages.</td></tr><tr><td>mail</td><td>Mail system.</td></tr><tr><td>daemon</td><td>System daemons.</td></tr></table>	Option	Description	kernel	Kernel messages.	user	Random user-level messages.	mail	Mail system.	daemon	System daemons.			
Option	Description													
kernel	Kernel messages.													
user	Random user-level messages.													
mail	Mail system.													
daemon	System daemons.													

Parameter	Description	Type	Size	Default																																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																												
	<i>auth</i>	Security/authorization messages.																																												
	<i>syslog</i>	Messages generated internally by syslog.																																												
	<i>lpr</i>	Line printer subsystem.																																												
	<i>news</i>	Network news subsystem.																																												
	<i>uucp</i>	Network news subsystem.																																												
	<i>cron</i>	Clock daemon.																																												
	<i>authpriv</i>	Security/authorization messages (private).																																												
	<i>ftp</i>	FTP daemon.																																												
	<i>ntp</i>	NTP daemon.																																												
	<i>audit</i>	Log audit.																																												
	<i>alert</i>	Log alert.																																												
	<i>clock</i>	Clock daemon.																																												
	<i>local0</i>	Reserved for local use.																																												
	<i>local1</i>	Reserved for local use.																																												
	<i>local2</i>	Reserved for local use.																																												
	<i>local3</i>	Reserved for local use.																																												
	<i>local4</i>	Reserved for local use.																																												
	<i>local5</i>	Reserved for local use.																																												
<i>local6</i>	Reserved for local use.																																													
<i>local7</i>	Reserved for local use.																																													
format	Log format.	option	-	default																																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.																																	
	Option	Description																																												
	<i>default</i>	Syslog format.																																												
	<i>csv</i>	CSV (Comma Separated Values) format.																																												
	<i>cef</i>	CEF (Common Event Format) format.																																												
	<i>rfc5424</i>	Syslog RFC5424 format.																																												
<i>json</i>	JSON (JavaScript Object Notation) format.																																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																																											

Parameter	Description	Type	Size	Default								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
Option	Description											
udp	Enable syslogging over UDP.											
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514								
priority	Set log transmission priority.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.					
Option	Description											
default	Set Syslog transmission priority to default.											
low	Set Syslog transmission priority to low.											
server	Address of remote syslog server.	string	Maximum length: 127									
source-ip	Source IP address of syslog.	string	Maximum length: 63									
source-ip-interface	Source interface of syslog.	string	Maximum length: 15									

Parameter	Description	Type	Size	Default														
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
status	Enable/disable remote syslog logging.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Log to remote syslog server.</td></tr><tr><td>disable</td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	enable	Log to remote syslog server.	disable	Do not log to remote syslog server.											
Option	Description																	
enable	Log to remote syslog server.																	
disable	Do not log to remote syslog server.																	
use-management-vdom	Enable/disable use of management VDOM as source VDOM for logs sent to syslog server.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of management VDOM as source VDOM.</td></tr><tr><td>disable</td><td>Use the current VDOM as source VDOM.</td></tr></table>	Option	Description	enable	Enable use of management VDOM as source VDOM.	disable	Use the current VDOM as source VDOM.											
Option	Description																	
enable	Enable use of management VDOM as source VDOM.																	
disable	Use the current VDOM as source VDOM.																	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0														

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log syslogd2 setting

Global settings for remote syslog server.

```

config log syslogd2 setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set source-ip-interface {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set vrf-select {integer}
end

```

config log syslogd2 setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable

Parameter	Description	Type	Size	Default																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>SSL communication with high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>SSL communication with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable SSL communication.</td></tr></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.																																							
	Option	Description																																																
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																																																
	<i>high</i>	SSL communication with high encryption algorithms.																																																
	<i>low</i>	SSL communication with low encryption algorithms.																																																
<i>disable</i>	Disable SSL communication.																																																	
facility	Remote syslog facility.	option	-	local7																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kernel</i></td><td>Kernel messages.</td></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.			
	Option	Description																																																
	<i>kernel</i>	Kernel messages.																																																
	<i>user</i>	Random user-level messages.																																																
	<i>mail</i>	Mail system.																																																
	<i>daemon</i>	System daemons.																																																
	<i>auth</i>	Security/authorization messages.																																																
	<i>syslog</i>	Messages generated internally by syslog.																																																
	<i>lpr</i>	Line printer subsystem.																																																
	<i>news</i>	Network news subsystem.																																																
	<i>uucp</i>	Network news subsystem.																																																
	<i>cron</i>	Clock daemon.																																																
	<i>authpriv</i>	Security/authorization messages (private).																																																
	<i>ftp</i>	FTP daemon.																																																
	<i>ntp</i>	NTP daemon.																																																
	<i>audit</i>	Log audit.																																																
	<i>alert</i>	Log alert.																																																
	<i>clock</i>	Clock daemon.																																																
	<i>local0</i>	Reserved for local use.																																																
	<i>local1</i>	Reserved for local use.																																																
	<i>local2</i>	Reserved for local use.																																																
<i>local3</i>	Reserved for local use.																																																	
<i>local4</i>	Reserved for local use.																																																	
<i>local5</i>	Reserved for local use.																																																	

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.									
	Option	Description														
	<i>local6</i>	Reserved for local use.														
<i>local7</i>	Reserved for local use.															
format	Log format.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.			
	Option	Description														
	<i>default</i>	Syslog format.														
	<i>csv</i>	CSV (Comma Separated Values) format.														
	<i>cef</i>	CEF (Common Event Format) format.														
	<i>rfc5424</i>	Syslog RFC5424 format.														
<i>json</i>	JSON (JavaScript Object Notation) format.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
	Option	Description														
	<i>auto</i>	Set outgoing interface automatically.														
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.														
<i>specify</i>	Set outgoing interface manually.															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).							
	Option	Description														
	<i>udp</i>	Enable syslogging over UDP.														
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).															

Parameter	Description	Type	Size	Default														
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514														
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.											
Option	Description																	
default	Set Syslog transmission priority to default.																	
low	Set Syslog transmission priority to low.																	
server	Address of remote syslog server.	string	Maximum length: 127															
source-ip	Source IP address of syslog.	string	Maximum length: 63															
source-ip-interface	Source interface of syslog.	string	Maximum length: 15															
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
status	Enable/disable remote syslog logging.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Log to remote syslog server.</td></tr><tr><td>disable</td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	enable	Log to remote syslog server.	disable	Do not log to remote syslog server.											
Option	Description																	
enable	Log to remote syslog server.																	
disable	Do not log to remote syslog server.																	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0														

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log syslogd3 filter

Filters for remote system server.

```
config log syslogd3 filter
  Description: Filters for remote system server.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end
```

config log syslogd3 filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
debug	Enable/disable debug logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Debug logging.		
	<i>disable</i>	Disable Debug logging.		
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Forti-Switch logging.		
	<i>disable</i>	Disable Forti-Switch logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config log syslogd3 override-filter

Override filters for remote system server.

```

config log syslogd3 override-filter
  Description: Override filters for remote system server.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end

```

config log syslogd3 override-filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
debug	Enable/disable debug logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Debug logging.		
	<i>disable</i>	Disable Debug logging.		
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Forti-Switch logging.		
	<i>disable</i>	Disable Forti-Switch logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config log syslogd3 override-setting

Override settings for remote syslog server.

```

config log syslogd3 override-setting
  Description: Override settings for remote syslog server.
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set custom {string}
      set name {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set max-log-rate {integer}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set priority [default|low]
  set server {string}
  set source-ip {string}
  set source-ip-interface {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
  set use-management-vdom [enable|disable]
  set vrf-select {integer}
end

```

config log syslogd3 override-setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option	Description		
	high-medium	SSL communication with high and medium encryption algorithms.		
	high	SSL communication with high encryption algorithms.		
	low	SSL communication with low encryption algorithms.		
	disable	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	Option	Description		
	kernel	Kernel messages.		
	user	Random user-level messages.		
	mail	Mail system.		
	daemon	System daemons.		
	auth	Security/authorization messages.		
	syslog	Messages generated internally by syslog.		
	lpr	Line printer subsystem.		
	news	Network news subsystem.		
	uucp	Network news subsystem.		
	cron	Clock daemon.		
	authpriv	Security/authorization messages (private).		
	ftp	FTP daemon.		
	ntp	NTP daemon.		
	audit	Log audit.		
	alert	Log alert.		
	clock	Clock daemon.		
	local0	Reserved for local use.		
local1	Reserved for local use.			

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																
	<i>local2</i>	Reserved for local use.																
	<i>local3</i>	Reserved for local use.																
	<i>local4</i>	Reserved for local use.																
	<i>local5</i>	Reserved for local use.																
	<i>local6</i>	Reserved for local use.																
<i>local7</i>	Reserved for local use.																	
format	Log format.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.					
	Option	Description																
	<i>default</i>	Syslog format.																
	<i>csv</i>	CSV (Comma Separated Values) format.																
	<i>cef</i>	CEF (Common Event Format) format.																
	<i>rfc5424</i>	Syslog RFC5424 format.																
<i>json</i>	JSON (JavaScript Object Notation) format.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.									
	Option	Description																
	<i>auto</i>	Set outgoing interface automatically.																
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																
<i>specify</i>	Set outgoing interface manually.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.													
	Option	Description																
<i>udp</i>	Enable syslogging over UDP.																	

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
	Option	Description																
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																	
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514														
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set Syslog transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.											
	Option	Description																
	<i>default</i>	Set Syslog transmission priority to default.																
<i>low</i>	Set Syslog transmission priority to low.																	
server	Address of remote syslog server.	string	Maximum length: 127															
source-ip	Source IP address of syslog.	string	Maximum length: 63															
source-ip-interface	Source interface of syslog.	string	Maximum length: 15															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
	Option	Description																
	<i>default</i>	Follow system global setting.																
	<i>SSLv3</i>	SSLv3.																
	<i>TLSv1</i>	TLSv1.																
	<i>TLSv1-1</i>	TLSv1.1.																
	<i>TLSv1-2</i>	TLSv1.2.																
<i>TLSv1-3</i>	TLSv1.3.																	
status	Enable/disable remote syslog logging.	option	-	disable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
use-management-vdom	Enable/disable use of management VDOM as source VDOM for logs sent to syslog server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of management VDOM as source VDOM.		
	<i>disable</i>	Use the current VDOM as source VDOM.		
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log syslogd3 setting

Global settings for remote syslog server.

```

config log syslogd3 setting
  Description: Global settings for remote syslog server.
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set custom {string}
      set name {string}
    next

```

```

end
set enc-algorithm [high-medium|high|...]
set facility [kernel|user|...]
set format [default|csv|...]
set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|legacy-reliable|...]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set source-ip-interface {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set vrf-select {integer}
end

```

config log syslogd3 setting

Parameter	Description	Type	Size	Default														
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high-medium</td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td>high</td><td>SSL communication with high encryption algorithms.</td></tr><tr><td>low</td><td>SSL communication with low encryption algorithms.</td></tr><tr><td>disable</td><td>Disable SSL communication.</td></tr></table>	Option	Description	high-medium	SSL communication with high and medium encryption algorithms.	high	SSL communication with high encryption algorithms.	low	SSL communication with low encryption algorithms.	disable	Disable SSL communication.							
Option	Description																	
high-medium	SSL communication with high and medium encryption algorithms.																	
high	SSL communication with high encryption algorithms.																	
low	SSL communication with low encryption algorithms.																	
disable	Disable SSL communication.																	
facility	Remote syslog facility.	option	-	local7														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>kernel</td><td>Kernel messages.</td></tr><tr><td>user</td><td>Random user-level messages.</td></tr><tr><td>mail</td><td>Mail system.</td></tr><tr><td>daemon</td><td>System daemons.</td></tr><tr><td>auth</td><td>Security/authorization messages.</td></tr><tr><td>syslog</td><td>Messages generated internally by syslog.</td></tr></table>	Option	Description	kernel	Kernel messages.	user	Random user-level messages.	mail	Mail system.	daemon	System daemons.	auth	Security/authorization messages.	syslog	Messages generated internally by syslog.			
Option	Description																	
kernel	Kernel messages.																	
user	Random user-level messages.																	
mail	Mail system.																	
daemon	System daemons.																	
auth	Security/authorization messages.																	
syslog	Messages generated internally by syslog.																	

Parameter	Description	Type	Size	Default																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																								
	<i>lpr</i>	Line printer subsystem.																																								
	<i>news</i>	Network news subsystem.																																								
	<i>uucp</i>	Network news subsystem.																																								
	<i>cron</i>	Clock daemon.																																								
	<i>authpriv</i>	Security/authorization messages (private).																																								
	<i>ftp</i>	FTP daemon.																																								
	<i>ntp</i>	NTP daemon.																																								
	<i>audit</i>	Log audit.																																								
	<i>alert</i>	Log alert.																																								
	<i>clock</i>	Clock daemon.																																								
	<i>local0</i>	Reserved for local use.																																								
	<i>local1</i>	Reserved for local use.																																								
	<i>local2</i>	Reserved for local use.																																								
	<i>local3</i>	Reserved for local use.																																								
	<i>local4</i>	Reserved for local use.																																								
	<i>local5</i>	Reserved for local use.																																								
	<i>local6</i>	Reserved for local use.																																								
	<i>local7</i>	Reserved for local use.																																								
format	Log format.	option	-	default																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.																													
	Option	Description																																								
	<i>default</i>	Syslog format.																																								
	<i>csv</i>	CSV (Comma Separated Values) format.																																								
	<i>cef</i>	CEF (Common Event Format) format.																																								
	<i>rfc5424</i>	Syslog RFC5424 format.																																								
<i>json</i>	JSON (JavaScript Object Notation) format.																																									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																																							

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option	Description		
	<i>udp</i>	Enable syslogging over UDP.		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		
server	Address of remote syslog server.	string	Maximum length: 127	
source-ip	Source IP address of syslog.	string	Maximum length: 63	
source-ip-interface	Source interface of syslog.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default														
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
	Option	Description																
	default	Follow system global setting.																
	SSLv3	SSLv3.																
	TLSv1	TLSv1.																
	TLSv1-1	TLSv1.1.																
	TLSv1-2	TLSv1.2.																
TLSv1-3	TLSv1.3.																	
status	Enable/disable remote syslog logging.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Log to remote syslog server.</td></tr><tr><td>disable</td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	enable	Log to remote syslog server.	disable	Do not log to remote syslog server.											
	Option	Description																
	enable	Log to remote syslog server.																
disable	Do not log to remote syslog server.																	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0														

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log syslogd4 filter

Filters for remote system server.

```

config log syslogd4 filter
    Description: Filters for remote system server.
    set anomaly [enable|disable]
    set debug [enable|disable]
    set forti-switch [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set http-transaction [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

config log syslogd4 filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									

Parameter	Description	Type	Size	Default								
forward-traffic	Enable/disable forward traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable forward traffic logging.</td></tr><tr><td>disable</td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	enable	Enable forward traffic logging.	disable	Disable forward traffic logging.					
Option	Description											
enable	Enable forward traffic logging.											
disable	Disable forward traffic logging.											
gtp *	Enable/disable GTP messages logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable GTP messages logging.</td></tr><tr><td>disable</td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	enable	Enable GTP messages logging.	disable	Disable GTP messages logging.					
Option	Description											
enable	Enable GTP messages logging.											
disable	Disable GTP messages logging.											
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable http transaction logging.</td></tr><tr><td>disable</td><td>Disable http transaction logging.</td></tr></table>	Option	Description	enable	Enable http transaction logging.	disable	Disable http transaction logging.					
Option	Description											
enable	Enable http transaction logging.											
disable	Disable http transaction logging.											
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable local in or out traffic logging.</td></tr><tr><td>disable</td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	enable	Enable local in or out traffic logging.	disable	Disable local in or out traffic logging.					
Option	Description											
enable	Enable local in or out traffic logging.											
disable	Disable local in or out traffic logging.											
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable multicast traffic logging.</td></tr><tr><td>disable</td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	enable	Enable multicast traffic logging.	disable	Disable multicast traffic logging.					
Option	Description											
enable	Enable multicast traffic logging.											
disable	Disable multicast traffic logging.											
severity	Lowest severity level to log.	option	-	information								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>emergency</td><td>Emergency level.</td></tr><tr><td>alert</td><td>Alert level.</td></tr><tr><td>critical</td><td>Critical level.</td></tr></table>	Option	Description	emergency	Emergency level.	alert	Alert level.	critical	Critical level.			
Option	Description											
emergency	Emergency level.											
alert	Alert level.											
critical	Critical level.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																																
	<i>attack</i>	Attack log.																																
	<i>spam</i>	Antispam log.																																
	<i>anomaly</i>	Anomaly log.																																
	<i>voip</i>	VoIP log.																																
	<i>dlp</i>	DLP log.																																
	<i>app-ctrl</i>	Application control log.																																
	<i>waf</i>	Web application firewall log.																																
	<i>dns</i>	DNS detail log.																																
	<i>ssh</i>	SSH log.																																
	<i>ssl</i>	SSL log.																																
	<i>file-filter</i>	File filter log.																																
	<i>icap</i>	ICAP log.																																
	<i>virtual-patch</i>	Virtual patch log.																																
<i>debug</i>	Debug log.																																	
filter	Free style filter string.	string	Maximum length: 1023																															
filter-type	Include/exclude logs that match the filter.	option	-	include																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																											
	Option	Description																																
	<i>include</i>	Include logs that match the filter.																																
<i>exclude</i>	Exclude logs that match the filter.																																	
id	Entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																															

config log syslogd4 override-filter

Override filters for remote system server.

```
config log syslogd4 override-filter
  Description: Override filters for remote system server.
  set anomaly [enable|disable]
  set debug [enable|disable]
```

```

set forti-switch [enable|disable]
set forward-traffic [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set http-transaction [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

config log syslogd4 override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr><tr><td><i>virtual-patch</i></td><td>Virtual patch log.</td></tr><tr><td><i>debug</i></td><td>Debug log.</td></tr></table>	Option	Description	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.	<i>debug</i>	Debug log.			
	Option	Description																												
	<i>anomaly</i>	Anomaly log.																												
	<i>voip</i>	VoIP log.																												
	<i>dlp</i>	DLP log.																												
	<i>app-ctrl</i>	Application control log.																												
	<i>waf</i>	Web application firewall log.																												
	<i>dns</i>	DNS detail log.																												
	<i>ssh</i>	SSH log.																												
	<i>ssl</i>	SSL log.																												
	<i>file-filter</i>	File filter log.																												
	<i>icap</i>	ICAP log.																												
	<i>virtual-patch</i>	Virtual patch log.																												
<i>debug</i>	Debug log.																													
filter	Free style filter string.	string	Maximum length: 1023																											
filter-type	Include/exclude logs that match the filter.	option	-	include																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																							
	Option	Description																												
	<i>include</i>	Include logs that match the filter.																												
<i>exclude</i>	Exclude logs that match the filter.																													
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295																											

config log syslogd4 override-setting

Override settings for remote syslog server.

```
config log syslogd4 override-setting
    Description: Override settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
```

```

        set name {string}
    next
end
set enc-algorithm [high-medium|high|...]
set facility [kernel|user|...]
set format [default|csv|...]
set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|legacy-reliable|...]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set source-ip-interface {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set use-management-vdom [enable|disable]
set vrf-select {integer}
end

```

config log syslogd4 override-setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option Description			
	high-medium	SSL communication with high and medium encryption algorithms.		
	high	SSL communication with high encryption algorithms.		
	low	SSL communication with low encryption algorithms.		
	disable	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	Option Description			
	kernel	Kernel messages.		
	user	Random user-level messages.		
	mail	Mail system.		
	daemon	System daemons.		

Parameter	Description	Type	Size	Default																																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																												
	<i>auth</i>	Security/authorization messages.																																												
	<i>syslog</i>	Messages generated internally by syslog.																																												
	<i>lpr</i>	Line printer subsystem.																																												
	<i>news</i>	Network news subsystem.																																												
	<i>uucp</i>	Network news subsystem.																																												
	<i>cron</i>	Clock daemon.																																												
	<i>authpriv</i>	Security/authorization messages (private).																																												
	<i>ftp</i>	FTP daemon.																																												
	<i>ntp</i>	NTP daemon.																																												
	<i>audit</i>	Log audit.																																												
	<i>alert</i>	Log alert.																																												
	<i>clock</i>	Clock daemon.																																												
	<i>local0</i>	Reserved for local use.																																												
	<i>local1</i>	Reserved for local use.																																												
	<i>local2</i>	Reserved for local use.																																												
	<i>local3</i>	Reserved for local use.																																												
	<i>local4</i>	Reserved for local use.																																												
	<i>local5</i>	Reserved for local use.																																												
<i>local6</i>	Reserved for local use.																																													
<i>local7</i>	Reserved for local use.																																													
format	Log format.	option	-	default																																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.																																	
	Option	Description																																												
	<i>default</i>	Syslog format.																																												
	<i>csv</i>	CSV (Comma Separated Values) format.																																												
	<i>cef</i>	CEF (Common Event Format) format.																																												
	<i>rfc5424</i>	Syslog RFC5424 format.																																												
<i>json</i>	JSON (JavaScript Object Notation) format.																																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																																											

Parameter	Description	Type	Size	Default								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
Option	Description											
udp	Enable syslogging over UDP.											
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514								
priority	Set log transmission priority.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.					
Option	Description											
default	Set Syslog transmission priority to default.											
low	Set Syslog transmission priority to low.											
server	Address of remote syslog server.	string	Maximum length: 127									
source-ip	Source IP address of syslog.	string	Maximum length: 63									
source-ip-interface	Source interface of syslog.	string	Maximum length: 15									

Parameter	Description	Type	Size	Default														
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
status	Enable/disable remote syslog logging.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Log to remote syslog server.</td></tr><tr><td>disable</td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	enable	Log to remote syslog server.	disable	Do not log to remote syslog server.											
Option	Description																	
enable	Log to remote syslog server.																	
disable	Do not log to remote syslog server.																	
use-management-vdom	Enable/disable use of management VDOM as source VDOM for logs sent to syslog server.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of management VDOM as source VDOM.</td></tr><tr><td>disable</td><td>Use the current VDOM as source VDOM.</td></tr></table>	Option	Description	enable	Enable use of management VDOM as source VDOM.	disable	Use the current VDOM as source VDOM.											
Option	Description																	
enable	Enable use of management VDOM as source VDOM.																	
disable	Use the current VDOM as source VDOM.																	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0														

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log syslogd4 setting

Global settings for remote syslog server.

```

config log syslogd4 setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set source-ip-interface {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set vrf-select {integer}
end

```

config log syslogd4 setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable

Parameter	Description	Type	Size	Default																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>SSL communication with high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>SSL communication with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable SSL communication.</td></tr></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.																																							
	Option	Description																																																
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																																																
	<i>high</i>	SSL communication with high encryption algorithms.																																																
	<i>low</i>	SSL communication with low encryption algorithms.																																																
<i>disable</i>	Disable SSL communication.																																																	
facility	Remote syslog facility.	option	-	local7																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kernel</i></td><td>Kernel messages.</td></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.			
	Option	Description																																																
	<i>kernel</i>	Kernel messages.																																																
	<i>user</i>	Random user-level messages.																																																
	<i>mail</i>	Mail system.																																																
	<i>daemon</i>	System daemons.																																																
	<i>auth</i>	Security/authorization messages.																																																
	<i>syslog</i>	Messages generated internally by syslog.																																																
	<i>lpr</i>	Line printer subsystem.																																																
	<i>news</i>	Network news subsystem.																																																
	<i>uucp</i>	Network news subsystem.																																																
	<i>cron</i>	Clock daemon.																																																
	<i>authpriv</i>	Security/authorization messages (private).																																																
	<i>ftp</i>	FTP daemon.																																																
	<i>ntp</i>	NTP daemon.																																																
	<i>audit</i>	Log audit.																																																
	<i>alert</i>	Log alert.																																																
	<i>clock</i>	Clock daemon.																																																
	<i>local0</i>	Reserved for local use.																																																
	<i>local1</i>	Reserved for local use.																																																
	<i>local2</i>	Reserved for local use.																																																
	<i>local3</i>	Reserved for local use.																																																
<i>local4</i>	Reserved for local use.																																																	
<i>local5</i>	Reserved for local use.																																																	

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.									
	Option	Description														
	<i>local6</i>	Reserved for local use.														
<i>local7</i>	Reserved for local use.															
format	Log format.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.			
	Option	Description														
	<i>default</i>	Syslog format.														
	<i>csv</i>	CSV (Comma Separated Values) format.														
	<i>cef</i>	CEF (Common Event Format) format.														
	<i>rfc5424</i>	Syslog RFC5424 format.														
<i>json</i>	JSON (JavaScript Object Notation) format.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
	Option	Description														
	<i>auto</i>	Set outgoing interface automatically.														
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.														
<i>specify</i>	Set outgoing interface manually.															
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).							
	Option	Description														
	<i>udp</i>	Enable syslogging over UDP.														
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).															

Parameter	Description	Type	Size	Default														
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514														
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.											
Option	Description																	
default	Set Syslog transmission priority to default.																	
low	Set Syslog transmission priority to low.																	
server	Address of remote syslog server.	string	Maximum length: 127															
source-ip	Source IP address of syslog.	string	Maximum length: 63															
source-ip-interface	Source interface of syslog.	string	Maximum length: 15															
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
status	Enable/disable remote syslog logging.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Log to remote syslog server.</td></tr><tr><td>disable</td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	enable	Log to remote syslog server.	disable	Do not log to remote syslog server.											
Option	Description																	
enable	Log to remote syslog server.																	
disable	Do not log to remote syslog server.																	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0														

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	

config log tacacs+accounting filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting filter
  Description: Settings for TACACS+ accounting events filter.
  set cli-cmd-audit [enable|disable]
  set config-change-audit [enable|disable]
  set login-audit [enable|disable]
end
```

config log tacacs+accounting filter

Parameter	Description	Type	Size	Default						
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for CLI commands audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for CLI commands audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.									
<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.									
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for configuration change events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for configuration change events audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.									
<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.									

Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for login events audit.		
	<i>disable</i>	Disable TACACS+ accounting for login events audit.		

config log tacacs+accounting setting

Settings for TACACS+ accounting.

```

config log tacacs+accounting setting
  Description: Settings for TACACS+ accounting.
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set server {string}
  set server-key {password}
  set source-ip {string}
  set status [enable|disable]
  set vrf-select {integer}
end

```

config log tacacs+accounting setting

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	

Parameter	Description	Type	Size	Default
source-ip	Source IP address for communication to TACACS+ server.	string	Maximum length: 63	
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option	Description		
	enable	Enable TACACS+ accounting.		
	disable	Disable TACACS+ accounting.		
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config log tacacs+accounting2 filter

Settings for TACACS+ accounting events filter.

```

config log tacacs+accounting2 filter
  Description: Settings for TACACS+ accounting events filter.
  set cli-cmd-audit [enable|disable]
  set config-change-audit [enable|disable]
  set login-audit [enable|disable]
end

```

config log tacacs+accounting2 filter

Parameter	Description	Type	Size	Default						
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for CLI commands audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for CLI commands audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.									
<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.									
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for configuration change events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for configuration change events audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.									
<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.									

Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for login events audit.		
	<i>disable</i>	Disable TACACS+ accounting for login events audit.		

config log tacacs+accounting2 setting

Settings for TACACS+ accounting.

```

config log tacacs+accounting2 setting
  Description: Settings for TACACS+ accounting.
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set server {string}
  set server-key {password}
  set source-ip {string}
  set status [enable|disable]
  set vrf-select {integer}
end

```

config log tacacs+accounting2 setting

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	

Parameter	Description	Type	Size	Default						
source-ip	Source IP address for communication to TACACS+ server.	string	Maximum length: 63							
status	Enable/disable TACACS+ accounting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting.	<i>disable</i>	Disable TACACS+ accounting.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting.									
<i>disable</i>	Disable TACACS+ accounting.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config log tacacs+accounting3 filter

Settings for TACACS+ accounting events filter.

```

config log tacacs+accounting3 filter
  Description: Settings for TACACS+ accounting events filter.
  set cli-cmd-audit [enable|disable]
  set config-change-audit [enable|disable]
  set login-audit [enable|disable]
end

```

config log tacacs+accounting3 filter

Parameter	Description	Type	Size	Default						
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for CLI commands audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for CLI commands audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.									
<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.									
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for configuration change events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for configuration change events audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.									
<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.									

Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for login events audit.		
	<i>disable</i>	Disable TACACS+ accounting for login events audit.		

config log tacacs+accounting3 setting

Settings for TACACS+ accounting.

```

config log tacacs+accounting3 setting
  Description: Settings for TACACS+ accounting.
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set server {string}
  set server-key {password}
  set source-ip {string}
  set status [enable|disable]
  set vrf-select {integer}
end

```

config log tacacs+accounting3 setting

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	

Parameter	Description	Type	Size	Default						
source-ip	Source IP address for communication to TACACS+ server.	string	Maximum length: 63							
status	Enable/disable TACACS+ accounting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting.	<i>disable</i>	Disable TACACS+ accounting.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting.									
<i>disable</i>	Disable TACACS+ accounting.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config log threat-weight

Configure threat weight settings.

```

config log threat-weight
    Description: Configure threat weight settings.
    config application
        Description: Application-control threat weight settings.
        edit <id>
            set category {integer}
            set level [disable|low|...]
        next
    end
    set blocked-connection [disable|low|...]
    set botnet-connection-detected [disable|low|...]
    set failed-connection [disable|low|...]
    config geolocation
        Description: Geolocation-based threat weight settings.
        edit <id>
            set country {string}
            set level [disable|low|...]
        next
    end
    config ips
        Description: IPS threat weight settings.
        set critical-severity [disable|low|...]
        set high-severity [disable|low|...]
        set info-severity [disable|low|...]
        set low-severity [disable|low|...]
        set medium-severity [disable|low|...]
    end
    config level
        Description: Score mapping for threat weight levels.

```

```

    set critical {integer}
    set high {integer}
    set low {integer}
    set medium {integer}
end
config malware
    Description: Anti-virus malware threat weight settings.
    set command-blocked [disable|low|...]
    set content-disarm [disable|low|...]
    set ems-threat-feed [disable|low|...]
    set file-blocked [disable|low|...]
    set fsa-high-risk [disable|low|...]
    set fsa-malicious [disable|low|...]
    set fsa-medium-risk [disable|low|...]
    set inline-block [disable|low|...]
    set malware-list [disable|low|...]
    set mimefragmented [disable|low|...]
    set oversized [disable|low|...]
    set switch-proto [disable|low|...]
    set virus-file-type-executable [disable|low|...]
    set virus-infected [disable|low|...]
    set virus-outbreak-prevention [disable|low|...]
    set virus-scan-error [disable|low|...]
end
set status [enable|disable]
set url-block-detected [disable|low|...]
config web
    Description: Web filtering threat weight settings.
    edit <id>
        set category {integer}
        set level [disable|low|...]
    next
end
end

```

config log threat-weight

Parameter	Description	Type	Size	Default
blocked-connection	Threat weight score for blocked connections.	option	-	high
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for blocked connections.		
	<i>low</i>	Use the low level score for blocked connections.		
	<i>medium</i>	Use the medium level score for blocked connections.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>Use the high level score for blocked connections.</td></tr><tr><td>critical</td><td>Use the critical level score for blocked connections.</td></tr></table>	Option	Description	high	Use the high level score for blocked connections.	critical	Use the critical level score for blocked connections.									
	Option	Description														
	high	Use the high level score for blocked connections.														
critical	Use the critical level score for blocked connections.															
botnet-connection-detected	Threat weight score for detected botnet connections.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for detected botnet connections.</td></tr><tr><td>low</td><td>Use the low level score for detected botnet connections.</td></tr><tr><td>medium</td><td>Use the medium level score for detected botnet connections.</td></tr><tr><td>high</td><td>Use the high level score for detected botnet connections.</td></tr><tr><td>critical</td><td>Use the critical level score for detected botnet connections.</td></tr></table>	Option	Description	disable	Disable threat weight scoring for detected botnet connections.	low	Use the low level score for detected botnet connections.	medium	Use the medium level score for detected botnet connections.	high	Use the high level score for detected botnet connections.	critical	Use the critical level score for detected botnet connections.			
	Option	Description														
	disable	Disable threat weight scoring for detected botnet connections.														
	low	Use the low level score for detected botnet connections.														
	medium	Use the medium level score for detected botnet connections.														
	high	Use the high level score for detected botnet connections.														
critical	Use the critical level score for detected botnet connections.															
failed-connection	Threat weight score for failed connections.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for failed connections.</td></tr><tr><td>low</td><td>Use the low level score for failed connections.</td></tr><tr><td>medium</td><td>Use the medium level score for failed connections.</td></tr><tr><td>high</td><td>Use the high level score for failed connections.</td></tr><tr><td>critical</td><td>Use the critical level score for failed connections.</td></tr></table>	Option	Description	disable	Disable threat weight scoring for failed connections.	low	Use the low level score for failed connections.	medium	Use the medium level score for failed connections.	high	Use the high level score for failed connections.	critical	Use the critical level score for failed connections.			
	Option	Description														
	disable	Disable threat weight scoring for failed connections.														
	low	Use the low level score for failed connections.														
	medium	Use the medium level score for failed connections.														
	high	Use the high level score for failed connections.														
critical	Use the critical level score for failed connections.															
status	Enable/disable the threat weight feature.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable the threat weight feature.</td></tr><tr><td>disable</td><td>Disable the threat weight feature.</td></tr></table>	Option	Description	enable	Enable the threat weight feature.	disable	Disable the threat weight feature.									
	Option	Description														
	enable	Enable the threat weight feature.														
disable	Disable the threat weight feature.															
url-block-detected	Threat weight score for URL blocking.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for URL blocking.</td></tr><tr><td>low</td><td>Use the low level score for URL blocking.</td></tr></table>	Option	Description	disable	Disable threat weight scoring for URL blocking.	low	Use the low level score for URL blocking.									
	Option	Description														
	disable	Disable threat weight scoring for URL blocking.														
low	Use the low level score for URL blocking.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>medium</i>	Use the medium level score for URL blocking.		
	<i>high</i>	Use the high level score for URL blocking.		
	<i>critical</i>	Use the critical level score for URL blocking.		

config application

Parameter	Description	Type	Size	Default
category	Application category.	integer	Minimum value: 0 Maximum value: 65535	0
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
level	Threat weight score for Application events.	option	-	low
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for Application events.		
	<i>low</i>	Use the low level score for Application events.		
	<i>medium</i>	Use the medium level score for Application events.		
	<i>high</i>	Use the high level score for Application events.		
	<i>critical</i>	Use the critical level score for Application events.		

config geolocation

Parameter	Description	Type	Size	Default
country	Country code.	string	Maximum length: 2	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
level	Threat weight score for Geolocation-based events.	option	-	low

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for Geolocation-based events.		
	<i>low</i>	Use the low level score for Geolocation-based events.		
	<i>medium</i>	Use the medium level score for Geolocation-based events.		
	<i>high</i>	Use the high level score for Geolocation-based events.		
	<i>critical</i>	Use the critical level score for Geolocation-based events.		

config ips

Parameter	Description	Type	Size	Default
critical-severity	Threat weight score for IPS critical severity events.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for IPS critical severity events.		
	<i>low</i>	Use the low level score for IPS critical severity events.		
	<i>medium</i>	Use the medium level score for IPS critical severity events.		
	<i>high</i>	Use the high level score for IPS critical severity events.		
	<i>critical</i>	Use the critical level score for IPS critical severity events.		
high-severity	Threat weight score for IPS high severity events.	option	-	high
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for IPS high severity events.		
	<i>low</i>	Use the low level score for IPS high severity events.		
	<i>medium</i>	Use the medium level score for IPS high severity events.		
	<i>high</i>	Use the high level score for IPS high severity events.		
	<i>critical</i>	Use the critical level score for IPS high severity events.		
info-severity	Threat weight score for IPS info severity events.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for IPS info severity events.		
	<i>low</i>	Use the low level score for IPS info severity events.		
	<i>medium</i>	Use the medium level score for IPS info severity events.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>Use the high level score for IPS info severity events.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for IPS info severity events.</td></tr></table>	Option	Description	<i>high</i>	Use the high level score for IPS info severity events.	<i>critical</i>	Use the critical level score for IPS info severity events.									
	Option	Description														
	<i>high</i>	Use the high level score for IPS info severity events.														
<i>critical</i>	Use the critical level score for IPS info severity events.															
low-severity	Threat weight score for IPS low severity events.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for IPS low severity events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for IPS low severity events.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for IPS low severity events.</td></tr><tr><td><i>high</i></td><td>Use the high level score for IPS low severity events.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for IPS low severity events.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for IPS low severity events.	<i>low</i>	Use the low level score for IPS low severity events.	<i>medium</i>	Use the medium level score for IPS low severity events.	<i>high</i>	Use the high level score for IPS low severity events.	<i>critical</i>	Use the critical level score for IPS low severity events.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for IPS low severity events.														
	<i>low</i>	Use the low level score for IPS low severity events.														
	<i>medium</i>	Use the medium level score for IPS low severity events.														
	<i>high</i>	Use the high level score for IPS low severity events.														
<i>critical</i>	Use the critical level score for IPS low severity events.															
medium-severity	Threat weight score for IPS medium severity events.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for IPS medium severity events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for IPS medium severity events.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for IPS medium severity events.</td></tr><tr><td><i>high</i></td><td>Use the high level score for IPS medium severity events.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for IPS medium severity events.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for IPS medium severity events.	<i>low</i>	Use the low level score for IPS medium severity events.	<i>medium</i>	Use the medium level score for IPS medium severity events.	<i>high</i>	Use the high level score for IPS medium severity events.	<i>critical</i>	Use the critical level score for IPS medium severity events.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for IPS medium severity events.														
	<i>low</i>	Use the low level score for IPS medium severity events.														
	<i>medium</i>	Use the medium level score for IPS medium severity events.														
	<i>high</i>	Use the high level score for IPS medium severity events.														
<i>critical</i>	Use the critical level score for IPS medium severity events.															

config level

Parameter	Description	Type	Size	Default
critical	Critical level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100	50
high	High level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100	30
low	Low level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100	5

Parameter	Description	Type	Size	Default
medium	Medium level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100	10

config malware

Parameter	Description	Type	Size	Default
command-blocked	Threat weight score for blocked command detected.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for blocked command detected.		
	<i>low</i>	Use the low level score for blocked command detected.		
	<i>medium</i>	Use the medium level score for blocked command detected.		
	<i>high</i>	Use the high level score for blocked command detected.		
	<i>critical</i>	Use the critical level score for blocked command detected.		
content-disarm	Threat weight score for virus (content disarm) detected.	option	-	medium
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus (content disarm) detected.		
	<i>low</i>	Use the low level score for virus (content disarm) detected.		
	<i>medium</i>	Use the medium level score for virus (content disarm) detected.		
	<i>high</i>	Use the high level score for virus (content disarm) detected.		
	<i>critical</i>	Use the critical level score for virus (content disarm) detected.		
ems-threat-feed	Threat weight score for virus (EMS threat feed) detected.	option	-	medium
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus (EMS threat feed) detected.		
	<i>low</i>	Use the low level score for virus (EMS threat feed) detected.		
	<i>medium</i>	Use the medium level score for virus (EMS threat feed) detected.		
	<i>high</i>	Use the high level score for virus (EMS threat feed) detected.		
	<i>critical</i>	Use the critical level score for virus (EMS threat feed) detected.		

Parameter	Description	Type	Size	Default
file-blocked	Threat weight score for blocked file detected.	option	-	low
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for blocked file detected.		
	<i>low</i>	Use the low level score for blocked file detected.		
	<i>medium</i>	Use the medium level score for blocked file detected.		
	<i>high</i>	Use the high level score for blocked file detected.		
	<i>critical</i>	Use the critical level score for blocked file detected.		
fsa-high-risk	Threat weight score for FortiSandbox high risk malware detected.	option	-	high
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for FortiSandbox high risk malware detected.		
	<i>low</i>	Use the low level score for FortiSandbox high risk malware detected.		
	<i>medium</i>	Use the medium level score for FortiSandbox high risk malware detected.		
	<i>high</i>	Use the high level score for FortiSandbox high risk malware detected.		
	<i>critical</i>	Use the critical level score for FortiSandbox high risk malware detected.		
fsa-malicious	Threat weight score for FortiSandbox malicious malware detected.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for FortiSandbox malicious malware detected.		
	<i>low</i>	Use the low level score for FortiSandbox malicious malware detected.		
	<i>medium</i>	Use the medium level score for FortiSandbox malicious malware detected.		
	<i>high</i>	Use the high level score for FortiSandbox malicious malware detected.		
	<i>critical</i>	Use the critical level score for FortiSandbox malicious malware detected.		

Parameter	Description	Type	Size	Default												
fsa-medium-risk	Threat weight score for FortiSandbox medium risk malware detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for FortiSandbox medium risk malware detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for FortiSandbox medium risk malware detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for FortiSandbox medium risk malware detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for FortiSandbox medium risk malware detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for FortiSandbox medium risk malware detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox medium risk malware detected.	<i>low</i>	Use the low level score for FortiSandbox medium risk malware detected.	<i>medium</i>	Use the medium level score for FortiSandbox medium risk malware detected.	<i>high</i>	Use the high level score for FortiSandbox medium risk malware detected.	<i>critical</i>	Use the critical level score for FortiSandbox medium risk malware detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for FortiSandbox medium risk malware detected.														
	<i>low</i>	Use the low level score for FortiSandbox medium risk malware detected.														
	<i>medium</i>	Use the medium level score for FortiSandbox medium risk malware detected.														
	<i>high</i>	Use the high level score for FortiSandbox medium risk malware detected.														
<i>critical</i>	Use the critical level score for FortiSandbox medium risk malware detected.															
inline-block	Threat weight score for malware detected by inline block.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus detected by inline block.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus detected by inline block.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus detected by inline block.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus detected by inline block.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus detected by inline block.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus detected by inline block.	<i>low</i>	Use the low level score for virus detected by inline block.	<i>medium</i>	Use the medium level score for virus detected by inline block.	<i>high</i>	Use the high level score for virus detected by inline block.	<i>critical</i>	Use the critical level score for virus detected by inline block.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus detected by inline block.														
	<i>low</i>	Use the low level score for virus detected by inline block.														
	<i>medium</i>	Use the medium level score for virus detected by inline block.														
	<i>high</i>	Use the high level score for virus detected by inline block.														
<i>critical</i>	Use the critical level score for virus detected by inline block.															
malware-list	Threat weight score for virus (malware list) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (malware list) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (malware list) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (malware list) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (malware list) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (malware list) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (malware list) detected.	<i>low</i>	Use the low level score for virus (malware list) detected.	<i>medium</i>	Use the medium level score for virus (malware list) detected.	<i>high</i>	Use the high level score for virus (malware list) detected.	<i>critical</i>	Use the critical level score for virus (malware list) detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus (malware list) detected.														
	<i>low</i>	Use the low level score for virus (malware list) detected.														
	<i>medium</i>	Use the medium level score for virus (malware list) detected.														
	<i>high</i>	Use the high level score for virus (malware list) detected.														
<i>critical</i>	Use the critical level score for virus (malware list) detected.															
mimefragmented	Threat weight score for mimefragmented detected.	option	-	disable												

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for mimefragmented detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for mimefragmented detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for mimefragmented detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for mimefragmented detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for mimefragmented detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for mimefragmented detected.	<i>low</i>	Use the low level score for mimefragmented detected.	<i>medium</i>	Use the medium level score for mimefragmented detected.	<i>high</i>	Use the high level score for mimefragmented detected.	<i>critical</i>	Use the critical level score for mimefragmented detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for mimefragmented detected.														
	<i>low</i>	Use the low level score for mimefragmented detected.														
	<i>medium</i>	Use the medium level score for mimefragmented detected.														
	<i>high</i>	Use the high level score for mimefragmented detected.														
	<i>critical</i>	Use the critical level score for mimefragmented detected.														
oversized	Threat weight score for oversized file detected.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for oversized file detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for oversized file detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for oversized file detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for oversized file detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for oversized file detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for oversized file detected.	<i>low</i>	Use the low level score for oversized file detected.	<i>medium</i>	Use the medium level score for oversized file detected.	<i>high</i>	Use the high level score for oversized file detected.	<i>critical</i>	Use the critical level score for oversized file detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for oversized file detected.														
	<i>low</i>	Use the low level score for oversized file detected.														
	<i>medium</i>	Use the medium level score for oversized file detected.														
	<i>high</i>	Use the high level score for oversized file detected.														
	<i>critical</i>	Use the critical level score for oversized file detected.														
switch-proto	Threat weight score for switch proto detected.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for switch proto detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for switch proto detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for switch proto detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for switch proto detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for switch proto detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for switch proto detected.	<i>low</i>	Use the low level score for switch proto detected.	<i>medium</i>	Use the medium level score for switch proto detected.	<i>high</i>	Use the high level score for switch proto detected.	<i>critical</i>	Use the critical level score for switch proto detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for switch proto detected.														
	<i>low</i>	Use the low level score for switch proto detected.														
	<i>medium</i>	Use the medium level score for switch proto detected.														
	<i>high</i>	Use the high level score for switch proto detected.														
	<i>critical</i>	Use the critical level score for switch proto detected.														
virus-file-type-executable	Threat weight score for virus (file type executable) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (filetype executable) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (filetype executable) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (filetype executable) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (filetype executable) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (filetype executable) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.	<i>low</i>	Use the low level score for virus (filetype executable) detected.	<i>medium</i>	Use the medium level score for virus (filetype executable) detected.	<i>high</i>	Use the high level score for virus (filetype executable) detected.	<i>critical</i>	Use the critical level score for virus (filetype executable) detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.														
	<i>low</i>	Use the low level score for virus (filetype executable) detected.														
	<i>medium</i>	Use the medium level score for virus (filetype executable) detected.														
	<i>high</i>	Use the high level score for virus (filetype executable) detected.														
	<i>critical</i>	Use the critical level score for virus (filetype executable) detected.														

Parameter	Description	Type	Size	Default
virus-infected	Threat weight score for virus (infected) detected.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus (infected) detected.		
	<i>low</i>	Use the low level score for virus (infected) detected.		
	<i>medium</i>	Use the medium level score for virus (infected) detected.		
	<i>high</i>	Use the high level score for virus (infected) detected.		
	<i>critical</i>	Use the critical level score for virus (infected) detected.		
virus-outbreak-prevention	Threat weight score for virus (outbreak prevention) event.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus (outbreak prevention) event.		
	<i>low</i>	Use the low level score for virus (outbreak prevention) event.		
	<i>medium</i>	Use the medium level score for virus (outbreak prevention) event.		
	<i>high</i>	Use the high level score for virus (outbreak prevention) event.		
	<i>critical</i>	Use the critical level score for virus (outbreak prevention) event.		
virus-scan-error	Threat weight score for virus (scan error) detected.	option	-	high
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus (scan error) detected.		
	<i>low</i>	Use the low level score for virus (scan error) detected.		
	<i>medium</i>	Use the medium level score for virus (scan error) detected.		
	<i>high</i>	Use the high level score for virus (scan error) detected.		
	<i>critical</i>	Use the critical level score for virus (scan error) detected.		

config web

Parameter	Description	Type	Size	Default
category	Threat weight score for web category filtering matches.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
level	Threat weight score for web category filtering matches.	option	-	low
	Option	Description		
	disable	Disable threat weight scoring for web category filtering matches.		
	low	Use the low level score for web category filtering matches.		
	medium	Use the medium level score for web category filtering matches.		
	high	Use the high level score for web category filtering matches.		
	critical	Use the critical level score for web category filtering matches.		

config log webtrends filter

Filters for WebTrends.

```
config log webtrends filter
  Description: Filters for WebTrends.
  set anomaly [enable|disable]
  set debug [enable|disable]
  set forti-switch [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set http-transaction [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end
```

config log webtrends filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
debug	Enable/disable debug logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Debug logging.</td></tr><tr><td><i>disable</i></td><td>Disable Debug logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Debug logging.	<i>disable</i>	Disable Debug logging.			
Option	Description									
<i>enable</i>	Enable Debug logging.									
<i>disable</i>	Disable Debug logging.									
forti-switch	Enable/disable Forti-Switch logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Switch logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Switch logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Switch logging.	<i>disable</i>	Disable Forti-Switch logging.			
Option	Description									
<i>enable</i>	Enable Forti-Switch logging.									
<i>disable</i>	Disable Forti-Switch logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
http-transaction	Enable/disable log HTTP transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log to WebTrends.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

* This parameter may not exist in some models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
	<i>debug</i>	Debug log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config log webtrends setting

Settings for WebTrends.

```
config log webtrends setting
    Description: Settings for WebTrends.
    set server {string}
    set status [enable|disable]
end
```

config log webtrends setting

Parameter	Description	Type	Size	Default
server	Address of the remote WebTrends server.	string	Maximum length: 63	
status	Enable/disable logging to WebTrends.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to WebTrends.		
	<i>disable</i>	Disable logging to WebTrends.		

monitoring

This section includes syntax for the following commands:

- [config monitoring np6-ipsec-engine on page 972](#)
- [config monitoring npu-hpe on page 973](#)

config monitoring np6-ipsec-engine



This command is available for model(s): FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D.

It is not available for: FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 3200F, FortiGate 3201F, FortiGate 3500F, FortiGate 3501F, FortiGate 3700F, FortiGate 3701F, FortiGate 400F, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NP6 IPsec engine status monitoring.

```
config monitoring np6-ipsec-engine
  Description: Configure NP6 IPsec engine status monitoring.
  set interval {integer}
  set status [enable|disable]
  set threshold {user}
end
```

config monitoring np6-ipsec-engine

Parameter	Description	Type	Size	Default
interval	IPsec engine status check interval (1 - 60 seconds, default = 1).	integer	Minimum value: 1 Maximum value: 60	1
status	Enable/disable NP6 IPsec engine status monitoring.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
threshold	IPsec engine status check threshold (x x x x x x x x, 8 integers from <1> to <255>, default = 15 15 12 12 8 8 5 5). Example: Log is generated if IPsec engine 0 is busy each of every 15 consecutive interval checks.	user	Not Specified	

config monitoring npu-hpe



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200F, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 120G, FortiGate 121G, FortiGate 200E, FortiGate 201E, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

Configure npu-hpe status monitoring.

```
config monitoring npu-hpe
  Description: Configure npu-hpe status monitoring.
  set interval {integer}
  set multipliers {user}
  set status [enable|disable]
end
```

config monitoring npu-hpe

Parameter	Description	Type	Size	Default						
interval	HPE status check interval (1 - 60 seconds, default = 1 second).	integer	Minimum value: 1 Maximum value: 60	1						
multipliers	HPE type interval multipliers (12 integers from <1> to <255>, default = 4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 8, 8). An event log is generated after every (interval * multiplier)seconds as configured for any HPE type when drops occur for that HPE type. An attack log is generated after every (4 * multiplier) number of continuous event logs.	user	Not Specified							
status	Enable/disable HPE status monitoring.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description									
enable	Enable setting.									
disable	Disable setting.									

nsxt

This section includes syntax for the following commands:

- [config nsxt service-chain on page 975](#)
- [config nsxt setting on page 977](#)

config nsxt service-chain



This command is available for model(s): FortiGate-VM64.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NSX-T service chain.

```
config nsxt service-chain
  Description: Configure NSX-T service chain.
  edit <id>
    set name {string}
    config service-index
      Description: Configure service index.
      edit <id>
        set name {string}
        set reverse-index {integer}
        set vd {string}
```

```
        next
    end
next
end
```

config nsxt service-chain

Parameter	Description	Type	Size	Default
id	Chain ID.	integer	Minimum value: 0 Maximum value: 1023	0
name	Chain name.	string	Maximum length: 63	

config service-index

Parameter	Description	Type	Size	Default
id	Service index.	integer	Minimum value: 0 Maximum value: 255	0
name	Index name.	string	Maximum length: 63	
reverse-index	Reverse service index.	integer	Minimum value: 1 Maximum value: 255	1
vd	VDOM name.	string	Maximum length: 31	

config nsxt setting



This command is available for model(s): FortiGate-VM64.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NSX-T setting.

```
config nsxt setting
    Description: Configure NSX-T setting.
    set liveness [enable|disable]
    set service {string}
end
```

config nsxt setting

Parameter	Description	Type	Size	Default
liveness	Enable/disable liveness detection packet forwarding.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable liveness detection packet forwarding.		
	<i>disable</i>	Disable liveness detection packet forwarding.		
service	Service name.	string	Maximum length: 63	

report

This section includes syntax for the following commands:

- [config report layout on page 978](#)
- [config report setting on page 987](#)

config report layout



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R.

Report layout configuration.

```
config report layout
  Description: Report layout configuration.
  edit <name>
    config body-item
      Description: Configure report body item.
      edit <id>
        set chart {string}
        set chart-options {option1}, {option2}, ...
        set content {string}
```

```

    set description {string}
    set img-src {string}
    set misc-component [hline|page-break|...]
    config parameters
        Description: Parameters.
        edit <id>
            set name {string}
            set value {string}
        next
    end
    set style {string}
    set text-component [text|heading1|...]
    set title {string}
    set top-n {integer}
    set type [text|image|...]
next
end
set cutoff-option [run-time|custom]
set cutoff-time {user}
set day [sunday|monday|...]
set description {string}
set email-recipients {string}
set email-send [enable|disable]
set format {option1}, {option2}, ...
set max-pdf-report {integer}
set options {option1}, {option2}, ...
config page
    Description: Configure report page.
    set column-break-before {option1}, {option2}, ...
    config footer
        Description: Configure report page footer.
        config footer-item
            Description: Configure report footer item.
            edit <id>
                set content {string}
                set description {string}
                set img-src {string}
                set style {string}
                set type [text|image]
            next
        end
        set style {string}
    end
config header
    Description: Configure report page header.
    config header-item
        Description: Configure report header item.
        edit <id>
            set content {string}
            set description {string}
            set img-src {string}
            set style {string}

```

```

        set type [text|image]
    next
    end
    set style {string}
end
set options {option1}, {option2}, ...
set page-break-before {option1}, {option2}, ...
set paper [a4|letter]
end
set schedule-type [demand|daily|...]
set style-theme {string}
set subtitle {string}
set time {user}
set title {string}
next
end

```

config report layout

Parameter	Description	Type	Size	Default
cutoff-option	Cutoff-option is either run-time or custom.	option	-	run-time
	Option Description			
	<i>run-time</i>	Run time.		
	<i>custom</i>	Custom.		
cutoff-time	Custom cutoff time to generate report (format = hh:mm).	user	Not Specified	
day	Schedule days of week to generate report.	option	-	sunday
	Option Description			
	<i>sunday</i>	Sunday.		
	<i>monday</i>	Monday.		
	<i>tuesday</i>	Tuesday.		
	<i>wednesday</i>	Wednesday.		
	<i>thursday</i>	Thursday.		
	<i>friday</i>	Friday.		
	<i>saturday</i>	Saturday.		
description	Description.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default												
email-recipients	Email recipients for generated reports.	string	Maximum length: 511													
email-send	Enable/disable sending emails after reports are generated.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending emails after generating reports.</td></tr><tr><td>disable</td><td>Disable sending emails after generating reports.</td></tr></table>	Option	Description	enable	Enable sending emails after generating reports.	disable	Disable sending emails after generating reports.									
Option	Description															
enable	Enable sending emails after generating reports.															
disable	Disable sending emails after generating reports.															
format	Report format.	option	-	pdf												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pdf</td><td>PDF.</td></tr></table>	Option	Description	pdf	PDF.											
Option	Description															
pdf	PDF.															
max-pdf-report	Maximum number of PDF reports to keep at one time (oldest report is overwritten).	integer	Minimum value: 1 Maximum value: 365	31												
name	Report layout name.	string	Maximum length: 35													
options	Report layout options.	option	-	include-table-of-content auto-numbering-heading view-chart-as-heading												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include-table-of-content</td><td>Include table of content in the report.</td></tr><tr><td>auto-numbering-heading</td><td>Prepend heading with auto numbering.</td></tr><tr><td>view-chart-as-heading</td><td>Auto add heading for each chart.</td></tr><tr><td>show-html-navbar-before-heading</td><td>Show HTML navigation bar before each heading.</td></tr><tr><td>dummy-option</td><td>Use this option if you need none of the above options.</td></tr></table>	Option	Description	include-table-of-content	Include table of content in the report.	auto-numbering-heading	Prepend heading with auto numbering.	view-chart-as-heading	Auto add heading for each chart.	show-html-navbar-before-heading	Show HTML navigation bar before each heading.	dummy-option	Use this option if you need none of the above options.			
Option	Description															
include-table-of-content	Include table of content in the report.															
auto-numbering-heading	Prepend heading with auto numbering.															
view-chart-as-heading	Auto add heading for each chart.															
show-html-navbar-before-heading	Show HTML navigation bar before each heading.															
dummy-option	Use this option if you need none of the above options.															

Parameter	Description	Type	Size	Default								
schedule-type	Report schedule type.	option	-	daily								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>demand</i></td><td>Run on demand.</td></tr><tr><td><i>daily</i></td><td>Schedule daily.</td></tr><tr><td><i>weekly</i></td><td>Schedule weekly.</td></tr></table>				Option	Description	<i>demand</i>	Run on demand.	<i>daily</i>	Schedule daily.	<i>weekly</i>	Schedule weekly.
	Option	Description										
	<i>demand</i>	Run on demand.										
	<i>daily</i>	Schedule daily.										
<i>weekly</i>	Schedule weekly.											
style-theme	Report style theme.	string	Maximum length: 35									
subtitle	Report subtitle.	string	Maximum length: 127									
time	Schedule time to generate report (format = hh:mm).	user	Not Specified									
title	Report title.	string	Maximum length: 127									

config body-item

Parameter	Description	Type	Size	Default								
chart	Report item chart name.	string	Maximum length: 71									
chart-options	Report chart options.	option	-	include-no-data hide-title show-caption								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include-no-data</i></td><td>Include chart with no data.</td></tr><tr><td><i>hide-title</i></td><td>Hide chart title.</td></tr><tr><td><i>show-caption</i></td><td>Show chart caption.</td></tr></table>				Option	Description	<i>include-no-data</i>	Include chart with no data.	<i>hide-title</i>	Hide chart title.	<i>show-caption</i>	Show chart caption.
	Option	Description										
	<i>include-no-data</i>	Include chart with no data.										
	<i>hide-title</i>	Hide chart title.										
<i>show-caption</i>	Show chart caption.											
content	Report item text content.	string	Maximum length: 511									
description	Description.	string	Maximum length: 63									

Parameter	Description	Type	Size	Default										
id	Report item ID.	integer	Minimum value: 0 0 Maximum value: 4294967295											
img-src	Report item image file name.	string	Maximum length: 127											
misc-component	Report item miscellaneous component.	option	-	hline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hline</td><td>Horizontal line.</td></tr><tr><td>page-break</td><td>Page break.</td></tr><tr><td>column-break</td><td>Column break.</td></tr><tr><td>section-start</td><td>Section start.</td></tr></table>				Option	Description	hline	Horizontal line.	page-break	Page break.	column-break	Column break.	section-start	Section start.
	Option	Description												
	hline	Horizontal line.												
	page-break	Page break.												
	column-break	Column break.												
section-start	Section start.													
style	Report item style.	string	Maximum length: 71											
text-component	Report item text component.	option	-	text										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>text</td><td>Normal text.</td></tr><tr><td>heading1</td><td>Heading 1.</td></tr><tr><td>heading2</td><td>Heading 2.</td></tr><tr><td>heading3</td><td>Heading 3.</td></tr></table>				Option	Description	text	Normal text.	heading1	Heading 1.	heading2	Heading 2.	heading3	Heading 3.
	Option	Description												
	text	Normal text.												
	heading1	Heading 1.												
	heading2	Heading 2.												
heading3	Heading 3.													
title	Report section title.	string	Maximum length: 511											
top-n	Value of top.	integer	Minimum value: 0 0 Maximum value: 4294967295											
type	Report item type.	option	-	text										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>text</td><td>Text.</td></tr><tr><td>image</td><td>Image.</td></tr><tr><td>chart</td><td>Chart.</td></tr><tr><td>misc</td><td>Miscellaneous.</td></tr></table>				Option	Description	text	Text.	image	Image.	chart	Chart.	misc	Miscellaneous.
	Option	Description												
	text	Text.												
	image	Image.												
	chart	Chart.												
misc	Miscellaneous.													

config parameters

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Field name that match field of parameters defined in dataset.	string	Maximum length: 127	
value	Value to replace corresponding field of parameters defined in dataset.	string	Maximum length: 1023	

config page

Parameter	Description	Type	Size	Default								
column-break-before	Report page auto column break before heading.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>heading1</td><td>Column break before heading 1.</td></tr><tr><td>heading2</td><td>Column break before heading 2.</td></tr><tr><td>heading3</td><td>Column break before heading 3.</td></tr></table>	Option	Description	heading1	Column break before heading 1.	heading2	Column break before heading 2.	heading3	Column break before heading 3.			
Option	Description											
heading1	Column break before heading 1.											
heading2	Column break before heading 2.											
heading3	Column break before heading 3.											
options	Report page options.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>header-on-first-page</td><td>Show header on first page.</td></tr><tr><td>footer-on-first-page</td><td>Show footer on first page.</td></tr></table>	Option	Description	header-on-first-page	Show header on first page.	footer-on-first-page	Show footer on first page.					
Option	Description											
header-on-first-page	Show header on first page.											
footer-on-first-page	Show footer on first page.											
page-break-before	Report page auto page break before heading.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>heading1</td><td>Page break before heading 1.</td></tr><tr><td>heading2</td><td>Page break before heading 2.</td></tr><tr><td>heading3</td><td>Page break before heading 3.</td></tr></table>	Option	Description	heading1	Page break before heading 1.	heading2	Page break before heading 2.	heading3	Page break before heading 3.			
Option	Description											
heading1	Page break before heading 1.											
heading2	Page break before heading 2.											
heading3	Page break before heading 3.											
paper	Report page paper.	option	-	a4								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>a4</i>	A4 paper.		
	<i>letter</i>	Letter paper.		

config footer

Parameter	Description	Type	Size	Default
style	Report footer style.	string	Maximum length: 71	

config footer-item

Parameter	Description	Type	Size	Default
content	Report item text content.	string	Maximum length: 511	
description	Description.	string	Maximum length: 63	
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	
img-src	Report item image file name.	string	Maximum length: 127	
style	Report item style.	string	Maximum length: 71	
type	Report item type.	option	-	text
	Option	Description		
	<i>text</i>	Text.		
	<i>image</i>	Image.		

config header

Parameter	Description	Type	Size	Default
style	Report header style.	string	Maximum length: 71	

config header-item

Parameter	Description	Type	Size	Default
content	Report item text content.	string	Maximum length: 511	
description	Description.	string	Maximum length: 63	
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	
img-src	Report item image file name.	string	Maximum length: 127	
style	Report item style.	string	Maximum length: 71	
type	Report item type.	option	-	text
	Option Description			
	<i>text</i>	Text.		
	<i>image</i>	Image.		

config report setting



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R.

Report setting configuration.

```
config report setting
  Description: Report setting configuration.
  set fortiview [enable|disable]
  set pdf-report [enable|disable]
  set report-source {option1}, {option2}, ...
  set top-n {integer}
  set web-browsing-threshold {integer}
end
```

config report setting

Parameter	Description	Type	Size	Default						
fortiview	Enable/disable historical FortiView.	option	-	enable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable historical FortiView.</td></tr><tr><td><i>disable</i></td><td>Disable historical FortiView.</td></tr></table>				Option	Description	<i>enable</i>	Enable historical FortiView.	<i>disable</i>	Disable historical FortiView.
Option	Description									
<i>enable</i>	Enable historical FortiView.									
<i>disable</i>	Disable historical FortiView.									

Parameter	Description	Type	Size	Default
pdf-report	Enable/disable PDF report.	option	-	enable **
	Option Description			
	<i>enable</i>	Enable PDF report.		
	<i>disable</i>	Disable PDF report.		
report-source	Report log source.	option	-	forward-traffic
	Option Description			
	<i>forward-traffic</i>	Report includes forward traffic logs.		
	<i>sniffer-traffic</i>	Report includes sniffer traffic logs.		
	<i>local-deny-traffic</i>	Report includes local deny traffic logs.		
top-n	Number of items to populate (1000 - 20000).	integer	Minimum value: 1000 Maximum value: 20000	1000
web-browsing-threshold	Web browsing time calculation threshold (3 - 15 min).	integer	Minimum value: 3 Maximum value: 15	3

** Values may differ between models.

router

This section includes syntax for the following commands:

- [config router access-list on page 989](#)
- [config router access-list6 on page 991](#)
- [config router aspath-list on page 992](#)
- [config router auth-path on page 993](#)
- [config router bfd on page 993](#)
- [config router bfd6 on page 995](#)
- [config router bgp on page 996](#)
- [config router community-list on page 1062](#)
- [config router extcommunity-list on page 1063](#)
- [config router isis on page 1064](#)
- [config router key-chain on page 1078](#)
- [config router multicast-flow on page 1092](#)
- [config router multicast on page 1079](#)
- [config router multicast6 on page 1090](#)
- [config router ospf on page 1093](#)
- [config router ospf6 on page 1110](#)
- [config router policy on page 1124](#)
- [config router policy6 on page 1127](#)
- [config router prefix-list on page 1130](#)
- [config router prefix-list6 on page 1131](#)
- [config router rip on page 1132](#)
- [config router ripng on page 1139](#)
- [config router route-map on page 1145](#)
- [config router setting on page 1151](#)
- [config router static on page 1152](#)
- [config router static6 on page 1154](#)

config router access-list

Configure access lists.

```
config router access-list
  Description: Configure access lists.
  edit <name>
    set comments {string}
    config rule
```

```

        Description: Rule.
    edit <id>
        set action [permit|deny]
        set exact-match [enable|disable]
        set prefix {user}
        set wildcard {user}
    next
end
next
end

```

config router access-list

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny this IP address and netmask prefix.	option	-	permit
	Option	Description		
	<i>permit</i>	Permit or allow this IP address and netmask prefix.		
	<i>deny</i>	Deny this IP address and netmask prefix.		
exact-match	Enable/disable exact match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable exact match.		
	<i>disable</i>	Disable exact match.		
id	Rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	
wildcard	Wildcard to define Cisco-style wildcard filter criteria.	user	Not Specified	

config router access-list6

Configure IPv6 access lists.

```
config router access-list6
  Description: Configure IPv6 access lists.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set exact-match [enable|disable]
        set flags {integer}
        set prefix6 {user}
      next
    end
  next
end
```

config router access-list6

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny this IP address and netmask prefix.	option	-	permit
	Option	Description		
	<i>permit</i>	Permit or allow this IP address and netmask prefix.		
	<i>deny</i>	Deny this IP address and netmask prefix.		
exact-match	Enable/disable exact prefix match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable exact match.		
	<i>disable</i>	Disable exact match.		

Parameter	Description	Type	Size	Default
flags	Flags. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	

config router aspath-list

Configure Autonomous System (AS) path lists.

```

config router aspath-list
  Description: Configure Autonomous System (AS) path lists.
  edit <name>
    config rule
      Description: AS path list rule.
      edit <id>
        set action [deny|permit]
        set regexp {string}
      next
    end
  next
end

```

config router aspath-list

Parameter	Description	Type	Size	Default
name	AS path list name.	string	Maximum length: 35	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny route-based operations, based on the route's AS_PATH attribute.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>deny</i>	Deny route-based operations.		
	<i>permit</i>	Permit route-based operations.		
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
regex	Regular-expression to match the Border Gateway Protocol (BGP) AS paths.	string	Maximum length: 63	

config router auth-path

Configure authentication based routing.

```
config router auth-path
  Description: Configure authentication based routing.
  edit <name>
    set device {string}
    set gateway {ipv4-address}
  next
end
```

config router auth-path

Parameter	Description	Type	Size	Default
device	Outgoing interface.	string	Maximum length: 35	
gateway	Gateway IP address.	ipv4-address	Not Specified	0.0.0.0
name	Name of the entry.	string	Maximum length: 15	

config router bfd

Configure BFD.

```
config router bfd
  Description: Configure BFD.
```

```

config multihop-template
  Description: BFD multi-hop template table.
  edit <id>
    set auth-mode [none|md5]
    set bfd-desired-min-tx {integer}
    set bfd-detect-mult {integer}
    set bfd-required-min-rx {integer}
    set dst {ipv4-classnet}
    set md5-key {password}
    set src {ipv4-classnet}
  next
end
config neighbor
  Description: Neighbor.
  edit <ip>
    set interface {string}
  next
end
end

```

config multihop-template

Parameter	Description	Type	Size	Default
auth-mode	Authentication mode.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>md5</i>	Meticulous MD5 mode.		
bfd-desired-min-tx	BFD desired minimal transmit interval (milliseconds).	integer	Minimum value: 100 Maximum value: 30000	250
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 3 Maximum value: 50	3
bfd-required-min-rx	BFD required minimal receive interval (milliseconds).	integer	Minimum value: 100 Maximum value: 30000	250
dst	Destination prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
md5-key	MD5 key of key ID 1.	password	Not Specified	

Parameter	Description	Type	Size	Default
src	Source prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config neighbor

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 15	
ip	IPv4 address of the BFD neighbor.	ipv4-address	Not Specified	0.0.0.0

config router bfd6

Configure IPv6 BFD.

```

config router bfd6
  Description: Configure IPv6 BFD.
  config multihop-template
    Description: BFD IPv6 multi-hop template table.
    edit <id>
      set auth-mode [none|md5]
      set bfd-desired-min-tx {integer}
      set bfd-detect-mult {integer}
      set bfd-required-min-rx {integer}
      set dst {ipv6-network}
      set md5-key {password}
      set src {ipv6-network}
    next
  end
  config neighbor
    Description: Configure neighbor of IPv6 BFD.
    edit <ip6-address>
      set interface {string}
    next
  end
end

```

config multihop-template

Parameter	Description	Type	Size	Default
auth-mode	Authentication mode.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	None.		
	<i>md5</i>	Meticulous MD5 mode.		
bfd-desired-min-tx	BFD desired minimal transmit interval (milliseconds).	integer	Minimum value: 100 Maximum value: 30000	250
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 3 Maximum value: 50	3
bfd-required-min-rx	BFD required minimal receive interval (milliseconds).	integer	Minimum value: 100 Maximum value: 30000	250
dst	Destination prefix.	ipv6-network	Not Specified	::/0
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
md5-key	MD5 key of key ID 1.	password	Not Specified	
src	Source prefix.	ipv6-network	Not Specified	::/0

config neighbor

Parameter	Description	Type	Size	Default
interface	Interface to the BFD neighbor.	string	Maximum length: 15	
ip6-address	IPv6 address of the BFD neighbor.	ipv6-address	Not Specified	::

config router bgp

Configure BGP.

```
config router bgp
  Description: Configure BGP.
  set additional-path [enable|disable]
  set additional-path-select {integer}
  set additional-path-select-vpnv4 {integer}
```

```

set additional-path-select-vpnv6 {integer}
set additional-path-select6 {integer}
set additional-path-vpnv4 [enable|disable]
set additional-path-vpnv6 [enable|disable]
set additional-path6 [enable|disable]
config admin-distance
    Description: Administrative distance modifications.
    edit <id>
        set distance {integer}
        set neighbour-prefix {ipv4-classnet}
        set route-list {string}
    next
end
config aggregate-address
    Description: BGP aggregate address table.
    edit <id>
        set as-set [enable|disable]
        set prefix {ipv4-classnet-any}
        set summary-only [enable|disable]
    next
end
config aggregate-address6
    Description: BGP IPv6 aggregate address table.
    edit <id>
        set as-set [enable|disable]
        set prefix6 {ipv6-prefix}
        set summary-only [enable|disable]
    next
end
set always-compare-med [enable|disable]
set as {user}
set bestpath-as-path-ignore [enable|disable]
set bestpath-cmp-confed-aspath [enable|disable]
set bestpath-cmp-routerid [enable|disable]
set bestpath-med-confed [enable|disable]
set bestpath-med-missing-as-worst [enable|disable]
set client-to-client-reflection [enable|disable]
set cluster-id {ipv4-address-any}
set confederation-identifier {integer}
set confederation-peers <peer1>, <peer2>, ...
set cross-family-conditional-adv [enable|disable]
set dampening [enable|disable]
set dampening-max-suppress-time {integer}
set dampening-reachability-half-life {integer}
set dampening-reuse {integer}
set dampening-route-map {string}
set dampening-suppress {integer}
set dampening-unreachability-half-life {integer}
set default-local-preference {integer}
set deterministic-med [enable|disable]
set distance-external {integer}
set distance-internal {integer}

```

```

set distance-local {integer}
set ebgp-multipath [enable|disable]
set enforce-first-as [enable|disable]
set fast-external-failover [enable|disable]
set graceful-end-on-timer [enable|disable]
set graceful-restart [enable|disable]
set graceful-restart-time {integer}
set graceful-stalepath-time {integer}
set graceful-update-delay {integer}
set holdtime-timer {integer}
set ibgp-multipath [enable|disable]
set ignore-optional-capability [enable|disable]
set keepalive-timer {integer}
set log-neighbour-changes [enable|disable]
set multipath-recursive-distance [enable|disable]
config neighbor
    Description: BGP neighbor table.
    edit <ip>
        set activate [enable|disable]
        set activate-evpn [enable|disable]
        set activate-vpnv4 [enable|disable]
        set activate-vpnv6 [enable|disable]
        set activate6 [enable|disable]
        set additional-path [send|receive|...]
        set additional-path-vpnv4 [send|receive|...]
        set additional-path-vpnv6 [send|receive|...]
        set additional-path6 [send|receive|...]
        set adv-additional-path {integer}
        set adv-additional-path-vpnv4 {integer}
        set adv-additional-path-vpnv6 {integer}
        set adv-additional-path6 {integer}
        set advertisement-interval {integer}
        set allowas-in {integer}
        set allowas-in-enable [enable|disable]
        set allowas-in-enable-evpn [enable|disable]
        set allowas-in-enable-vpnv4 [enable|disable]
        set allowas-in-enable-vpnv6 [enable|disable]
        set allowas-in-enable6 [enable|disable]
        set allowas-in-evpn {integer}
        set allowas-in-vpnv4 {integer}
        set allowas-in-vpnv6 {integer}
        set allowas-in6 {integer}
        set as-override [enable|disable]
        set as-override6 [enable|disable]
        set attribute-unchanged {option1}, {option2}, ...
        set attribute-unchanged-vpnv4 {option1}, {option2}, ...
        set attribute-unchanged-vpnv6 {option1}, {option2}, ...
        set attribute-unchanged6 {option1}, {option2}, ...
        set auth-options {string}
        set bfd [enable|disable]
        set capability-default-originate [enable|disable]
        set capability-default-originate6 [enable|disable]

```

```

set capability-dynamic [enable|disable]
set capability-graceful-restart [enable|disable]
set capability-graceful-restart-evpn [enable|disable]
set capability-graceful-restart-vpnv4 [enable|disable]
set capability-graceful-restart-vpnv6 [enable|disable]
set capability-graceful-restart6 [enable|disable]
set capability-orf [none|receive|...]
set capability-orf6 [none|receive|...]
set capability-route-refresh [enable|disable]
config conditional-advertise
    Description: Conditional advertisement.
    edit <advertise-routemap>
        set condition-routemap <name1>, <name2>, ...
        set condition-type [exist|non-exist]
    next
end
config conditional-advertise6
    Description: IPv6 conditional advertisement.
    edit <advertise-routemap>
        set condition-routemap <name1>, <name2>, ...
        set condition-type [exist|non-exist]
    next
end
set connect-timer {integer}
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in-vpnv4 {string}
set distribute-list-in-vpnv6 {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out-vpnv4 {string}
set distribute-list-out-vpnv6 {string}
set distribute-list-out6 {string}
set dont-capability-negotiate [enable|disable]
set ebgp-enforce-multihop [enable|disable]
set ebgp-multihop-ttl {integer}
set filter-list-in {string}
set filter-list-in-vpnv4 {string}
set filter-list-in-vpnv6 {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out-vpnv4 {string}
set filter-list-out-vpnv6 {string}
set filter-list-out6 {string}
set holdtime-timer {integer}
set interface {string}
set keep-alive-timer {integer}
set link-down-failover [enable|disable]
set local-as {user}
set local-as-no-prepend [enable|disable]

```

```
set local-as-replace-as [enable|disable]
set maximum-prefix {integer}
set maximum-prefix-evpn {integer}
set maximum-prefix-threshold {integer}
set maximum-prefix-threshold-evpn {integer}
set maximum-prefix-threshold-vpnv4 {integer}
set maximum-prefix-threshold-vpnv6 {integer}
set maximum-prefix-threshold6 {integer}
set maximum-prefix-vpnv4 {integer}
set maximum-prefix-vpnv6 {integer}
set maximum-prefix-warning-only [enable|disable]
set maximum-prefix-warning-only-evpn [enable|disable]
set maximum-prefix-warning-only-vpnv4 [enable|disable]
set maximum-prefix-warning-only-vpnv6 [enable|disable]
set maximum-prefix-warning-only6 [enable|disable]
set maximum-prefix6 {integer}
set next-hop-self [enable|disable]
set next-hop-self-rr [enable|disable]
set next-hop-self-rr6 [enable|disable]
set next-hop-self-vpnv4 [enable|disable]
set next-hop-self-vpnv6 [enable|disable]
set next-hop-self6 [enable|disable]
set override-capability [enable|disable]
set passive [enable|disable]
set password {password}
set prefix-list-in {string}
set prefix-list-in-vpnv4 {string}
set prefix-list-in-vpnv6 {string}
set prefix-list-in6 {string}
set prefix-list-out {string}
set prefix-list-out-vpnv4 {string}
set prefix-list-out-vpnv6 {string}
set prefix-list-out6 {string}
set remote-as {user}
set remove-private-as [enable|disable]
set remove-private-as-evpn [enable|disable]
set remove-private-as-vpnv4 [enable|disable]
set remove-private-as-vpnv6 [enable|disable]
set remove-private-as6 [enable|disable]
set restart-time {integer}
set retain-stale-time {integer}
set route-map-in {string}
set route-map-in-evpn {string}
set route-map-in-vpnv4 {string}
set route-map-in-vpnv6 {string}
set route-map-in6 {string}
set route-map-out {string}
set route-map-out-evpn {string}
set route-map-out-preferable {string}
set route-map-out-vpnv4 {string}
set route-map-out-vpnv4-preferable {string}
set route-map-out-vpnv6 {string}
```



```

    set route-map-out-vpnv6-preferable {string}
    set route-map-out6 {string}
    set route-map-out6-preferable {string}
    set route-reflector-client [enable|disable]
    set route-reflector-client-evpn [enable|disable]
    set route-reflector-client-vpnv4 [enable|disable]
    set route-reflector-client-vpnv6 [enable|disable]
    set route-reflector-client6 [enable|disable]
    set route-server-client [enable|disable]
    set route-server-client-evpn [enable|disable]
    set route-server-client-vpnv4 [enable|disable]
    set route-server-client-vpnv6 [enable|disable]
    set route-server-client6 [enable|disable]
    set rr-attr-allow-change [enable|disable]
    set rr-attr-allow-change-evpn [enable|disable]
    set rr-attr-allow-change-vpnv4 [enable|disable]
    set rr-attr-allow-change-vpnv6 [enable|disable]
    set rr-attr-allow-change6 [enable|disable]
    set send-community [standard|extended|...]
    set send-community-evpn [standard|extended|...]
    set send-community-vpnv4 [standard|extended|...]
    set send-community-vpnv6 [standard|extended|...]
    set send-community6 [standard|extended|...]
    set shutdown [enable|disable]
    set soft-reconfiguration [enable|disable]
    set soft-reconfiguration-evpn [enable|disable]
    set soft-reconfiguration-vpnv4 [enable|disable]
    set soft-reconfiguration-vpnv6 [enable|disable]
    set soft-reconfiguration6 [enable|disable]
    set stale-route [enable|disable]
    set strict-capability-match [enable|disable]
    set unsuppress-map {string}
    set unsuppress-map6 {string}
    set update-source {string}
    set weight {integer}
next
end
config neighbor-group
    Description: BGP neighbor group table.
    edit <name>
        set activate [enable|disable]
        set activate-evpn [enable|disable]
        set activate-vpnv4 [enable|disable]
        set activate-vpnv6 [enable|disable]
        set activate6 [enable|disable]
        set additional-path [send|receive|...]
        set additional-path-vpnv4 [send|receive|...]
        set additional-path-vpnv6 [send|receive|...]
        set additional-path6 [send|receive|...]
        set adv-additional-path {integer}
        set adv-additional-path-vpnv4 {integer}
        set adv-additional-path-vpnv6 {integer}

```

```

set adv-additional-path6 {integer}
set advertisement-interval {integer}
set allowas-in {integer}
set allowas-in-enable [enable|disable]
set allowas-in-enable-evpn [enable|disable]
set allowas-in-enable-vpnv4 [enable|disable]
set allowas-in-enable-vpnv6 [enable|disable]
set allowas-in-enable6 [enable|disable]
set allowas-in-evpn {integer}
set allowas-in-vpnv4 {integer}
set allowas-in-vpnv6 {integer}
set allowas-in6 {integer}
set as-override [enable|disable]
set as-override6 [enable|disable]
set attribute-unchanged {option1}, {option2}, ...
set attribute-unchanged-vpnv4 {option1}, {option2}, ...
set attribute-unchanged-vpnv6 {option1}, {option2}, ...
set attribute-unchanged6 {option1}, {option2}, ...
set auth-options {string}
set bfd [enable|disable]
set capability-default-originate [enable|disable]
set capability-default-originate6 [enable|disable]
set capability-dynamic [enable|disable]
set capability-graceful-restart [enable|disable]
set capability-graceful-restart-evpn [enable|disable]
set capability-graceful-restart-vpnv4 [enable|disable]
set capability-graceful-restart-vpnv6 [enable|disable]
set capability-graceful-restart6 [enable|disable]
set capability-orf [none|receive|...]
set capability-orf6 [none|receive|...]
set capability-route-refresh [enable|disable]
set connect-timer {integer}
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in-vpnv4 {string}
set distribute-list-in-vpnv6 {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out-vpnv4 {string}
set distribute-list-out-vpnv6 {string}
set distribute-list-out6 {string}
set dont-capability-negotiate [enable|disable]
set ebgp-enforce-multihop [enable|disable]
set ebgp-multihop-ttl {integer}
set filter-list-in {string}
set filter-list-in-vpnv4 {string}
set filter-list-in-vpnv6 {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out-vpnv4 {string}

```

```
set filter-list-out-vpnv6 {string}
set filter-list-out6 {string}
set holdtime-timer {integer}
set interface {string}
set keep-alive-timer {integer}
set link-down-failover [enable|disable]
set local-as {user}
set local-as-no-prepend [enable|disable]
set local-as-replace-as [enable|disable]
set maximum-prefix {integer}
set maximum-prefix-evpn {integer}
set maximum-prefix-threshold {integer}
set maximum-prefix-threshold-evpn {integer}
set maximum-prefix-threshold-vpnv4 {integer}
set maximum-prefix-threshold-vpnv6 {integer}
set maximum-prefix-threshold6 {integer}
set maximum-prefix-vpnv4 {integer}
set maximum-prefix-vpnv6 {integer}
set maximum-prefix-warning-only [enable|disable]
set maximum-prefix-warning-only-evpn [enable|disable]
set maximum-prefix-warning-only-vpnv4 [enable|disable]
set maximum-prefix-warning-only-vpnv6 [enable|disable]
set maximum-prefix-warning-only6 [enable|disable]
set maximum-prefix6 {integer}
set next-hop-self [enable|disable]
set next-hop-self-rr [enable|disable]
set next-hop-self-rr6 [enable|disable]
set next-hop-self-vpnv4 [enable|disable]
set next-hop-self-vpnv6 [enable|disable]
set next-hop-self6 [enable|disable]
set override-capability [enable|disable]
set passive [enable|disable]
set password {password}
set prefix-list-in {string}
set prefix-list-in-vpnv4 {string}
set prefix-list-in-vpnv6 {string}
set prefix-list-in6 {string}
set prefix-list-out {string}
set prefix-list-out-vpnv4 {string}
set prefix-list-out-vpnv6 {string}
set prefix-list-out6 {string}
set remote-as {user}
set remote-as-filter {string}
set remove-private-as [enable|disable]
set remove-private-as-evpn [enable|disable]
set remove-private-as-vpnv4 [enable|disable]
set remove-private-as-vpnv6 [enable|disable]
set remove-private-as6 [enable|disable]
set restart-time {integer}
set retain-stale-time {integer}
set route-map-in {string}
set route-map-in-evpn {string}
```

```

    set route-map-in-vpnv4 {string}
    set route-map-in-vpnv6 {string}
    set route-map-in6 {string}
    set route-map-out {string}
    set route-map-out-evpn {string}
    set route-map-out-preferable {string}
    set route-map-out-vpnv4 {string}
    set route-map-out-vpnv4-preferable {string}
    set route-map-out-vpnv6 {string}
    set route-map-out-vpnv6-preferable {string}
    set route-map-out6 {string}
    set route-map-out6-preferable {string}
    set route-reflector-client [enable|disable]
    set route-reflector-client-evpn [enable|disable]
    set route-reflector-client-vpnv4 [enable|disable]
    set route-reflector-client-vpnv6 [enable|disable]
    set route-reflector-client6 [enable|disable]
    set route-server-client [enable|disable]
    set route-server-client-evpn [enable|disable]
    set route-server-client-vpnv4 [enable|disable]
    set route-server-client-vpnv6 [enable|disable]
    set route-server-client6 [enable|disable]
    set rr-attr-allow-change [enable|disable]
    set rr-attr-allow-change-evpn [enable|disable]
    set rr-attr-allow-change-vpnv4 [enable|disable]
    set rr-attr-allow-change-vpnv6 [enable|disable]
    set rr-attr-allow-change6 [enable|disable]
    set send-community [standard|extended|...]
    set send-community-evpn [standard|extended|...]
    set send-community-vpnv4 [standard|extended|...]
    set send-community-vpnv6 [standard|extended|...]
    set send-community6 [standard|extended|...]
    set shutdown [enable|disable]
    set soft-reconfiguration [enable|disable]
    set soft-reconfiguration-evpn [enable|disable]
    set soft-reconfiguration-vpnv4 [enable|disable]
    set soft-reconfiguration-vpnv6 [enable|disable]
    set soft-reconfiguration6 [enable|disable]
    set stale-route [enable|disable]
    set strict-capability-match [enable|disable]
    set unsuppress-map {string}
    set unsuppress-map6 {string}
    set update-source {string}
    set weight {integer}
next
end
config neighbor-range
    Description: BGP neighbor range table.
    edit <id>
        set max-neighbor-num {integer}
        set neighbor-group {string}
        set prefix {ipv4-classnet}

```

```

    next
end
config neighbor-range6
    Description: BGP IPv6 neighbor range table.
    edit <id>
        set max-neighbor-num {integer}
        set neighbor-group {string}
        set prefix6 {ipv6-network}
    next
end
config network
    Description: BGP network table.
    edit <id>
        set backdoor [enable|disable]
        set network-import-check [global|enable|...]
        set prefix {ipv4-classnet}
        set prefix-name {string}
        set route-map {string}
    next
end
set network-import-check [enable|disable]
config network6
    Description: BGP IPv6 network table.
    edit <id>
        set backdoor [enable|disable]
        set network-import-check [global|enable|...]
        set prefix6 {ipv6-network}
        set route-map {string}
    next
end
set recursive-inherit-priority [enable|disable]
set recursive-next-hop [enable|disable]
config redistribute
    Description: BGP IPv4 redistribute table. Read-only.
    edit <name>
        set route-map {string}
        set status [enable|disable]
    next
end
config redistribute6
    Description: BGP IPv6 redistribute table. Read-only.
    edit <name>
        set route-map {string}
        set status [enable|disable]
    next
end
set router-id {ipv4-address-any}
set scan-time {integer}
set synchronization [enable|disable]
set tag-resolve-mode [disable|preferred|...]
config vrf
    Description: BGP VRF leaking table.

```

```

edit <vrf>
    set export-rt <route-target1>, <route-target2>, ...
    set import-route-map {string}
    set import-rt <route-target1>, <route-target2>, ...
    config leak-target
        Description: Target VRF table.
        edit <vrf>
            set interface {string}
            set route-map {string}
        next
    end
    set rd {string}
    set role [standalone|ce|...]
next
end
config vrf6
    Description: BGP IPv6 VRF leaking table.
    edit <vrf>
        set export-rt <route-target1>, <route-target2>, ...
        set import-route-map {string}
        set import-rt <route-target1>, <route-target2>, ...
        config leak-target
            Description: Target VRF table.
            edit <vrf>
                set interface {string}
                set route-map {string}
            next
        end
        set rd {string}
        set role [standalone|ce|...]
    next
end
end

```

config router bgp

Parameter	Description	Type	Size	Default
additional-path	Enable/disable selection of BGP IPv4 additional paths.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
additional-path-select	Number of additional paths to be selected for each IPv4 NLRI.	integer	Minimum value: 2 Maximum value: 255	2

Parameter	Description	Type	Size	Default						
additional-path-select-vpnv4	Number of additional paths to be selected for each VPNv4 NLRI.	integer	Minimum value: 2 2 Maximum value: 255	2						
additional-path-select-vpnv6	Number of additional paths to be selected for each VPNv6 NLRI.	integer	Minimum value: 2 2 Maximum value: 255	2						
additional-path-select6	Number of additional paths to be selected for each IPv6 NLRI.	integer	Minimum value: 2 2 Maximum value: 255	2						
additional-path-vpnv4	Enable/disable selection of BGP VPNv4 additional paths.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
additional-path-vpnv6	Enable/disable selection of BGP VPNv6 additional paths.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
additional-path6	Enable/disable selection of BGP IPv6 additional paths.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
always-compare-med	Enable/disable always compare MED.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as	Router AS number, asplain/asdot/asdot+ format, 0 to disable BGP.	user	Not Specified							
bestpath-as-path-ignore	Enable/disable ignore AS path.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-cmp-confed-aspath	Enable/disable compare federation AS path length.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-cmp-routerid	Enable/disable compare router ID for identical EBGP paths.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-med-confed	Enable/disable compare MED among confederation paths.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-med-missing-as-worst	Enable/disable treat missing MED as least preferred.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
client-to-client-reflection	Enable/disable client-to-client route reflection.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
cluster-id	Route reflector cluster ID.	ipv4-address-any	Not Specified	0.0.0.0
confederation-identifier	Confederation identifier.	integer	Minimum value: 0 1 Maximum value: 4294967295	0
confederation-peers <peer>	Confederation peers. Peer ID.	string	Maximum length: 79	
cross-family-conditional-adv	Enable/disable cross address family conditional advertisement.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
dampening	Enable/disable route-flap dampening.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
dampening-max-suppress-time	Maximum minutes a route can be suppressed.	integer	Minimum value: 60 1 Maximum value: 255	60
dampening-reachability-half-life	Reachability half-life time for penalty (min).	integer	Minimum value: 15 1 Maximum value: 45	15
dampening-reuse	Threshold to reuse routes.	integer	Minimum value: 750 1 Maximum value: 20000	750
dampening-route-map	Criteria for dampening.	string	Maximum length: 35	
dampening-suppress	Threshold to suppress routes.	integer	Minimum value: 2000 1 Maximum value: 20000	2000
dampening-unreachability-half-life	Unreachability half-life time for penalty (min).	integer	Minimum value: 15 1 Maximum value: 45	15

Parameter	Description	Type	Size	Default						
default-local-preference	Default local preference.	integer	Minimum value: 0 Maximum value: 4294967295	100						
deterministic-med	Enable/disable enforce deterministic comparison of MED.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
distance-external	Distance for routes external to the AS.	integer	Minimum value: 1 Maximum value: 255	20						
distance-internal	Distance for routes internal to the AS.	integer	Minimum value: 1 Maximum value: 255	200						
distance-local	Distance for routes local to the AS.	integer	Minimum value: 1 Maximum value: 255	200						
ebgp-multipath	Enable/disable EBGp multi-path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
enforce-first-as	Enable/disable enforce first AS for EBGp routes.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
fast-external-failover	Enable/disable reset peer BGP session if link goes down.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
graceful-end-on-timer	Enable/disable to exit graceful restart on timer only.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
graceful-restart	Enable/disable BGP graceful restart capabilities.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
graceful-restart-time	Time needed for neighbors to restart (sec).	integer	Minimum value: 120 1 Maximum value: 3600							
graceful-stalepath-time	Time to hold stale paths of restarting neighbor (sec).	integer	Minimum value: 360 1 Maximum value: 3600							
graceful-update-delay	Route advertisement/selection delay after restart (sec).	integer	Minimum value: 120 1 Maximum value: 3600							
holdtime-timer	Number of seconds to mark peer as dead.	integer	Minimum value: 180 3 Maximum value: 65535							
ibgp-multipath	Enable/disable IBGP multi-path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ignore-optional-capability	Do not send unknown optional capability notification message.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
keepalive-timer	Frequency to send keep alive requests.	integer	Minimum value: 0 Maximum value: 65535	60						
log-neighbour-changes	Log BGP neighbor changes.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
multipath-recursive-distance	Enable/disable use of recursive distance to select multipath.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
network-import-check	Enable/disable ensure BGP network route exists in IGP.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
recursive-inherit-priority	Enable/disable priority inheritance for recursive resolution.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
recursive-next-hop	Enable/disable recursive resolution of next-hop using BGP route.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
router-id	Router ID.	ipv4-address-any	Not Specified							

Parameter	Description	Type	Size	Default
scan-time	Background scanner interval (sec), 0 to disable it.	integer	Minimum value: 5 Maximum value: 60	60
synchronization	Enable/disable only advertise routes from iBGP if routes present in an IGP.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
tag-resolve-mode	Configure tag-match mode. Resolves BGP routes with other routes containing the same tag.	option	-	disable
	Option	Description		
	disable	Disable tag-match mode.		
	preferred	Use tag-match if a BGP route resolution with another route containing the same tag is successful.		
	merge	Merge tag-match with best-match if they are using different routes. The result will exclude the next hops of tag-match whose interfaces or child interfaces have appeared in best-match.		
	merge-all	Merge tag-match with best-match if they are using different routes. The result will exclude the next hops of tag-match whose interfaces have appeared in best-match.		

config admin-distance

Parameter	Description	Type	Size	Default
distance	Administrative distance to apply (1 - 255).	integer	Minimum value: 1 Maximum value: 255	0
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
neighbour-prefix	Neighbor address prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
route-list	Access list of routes to apply new distance to.	string	Maximum length: 35	

config aggregate-address

Parameter	Description	Type	Size	Default
as-set	Enable/disable generate AS set path information.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Aggregate prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
summary-only	Enable/disable filter more specific routes from updates.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	

config aggregate-address6

Parameter	Description	Type	Size	Default
as-set	Enable/disable generate AS set path information.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	Aggregate IPv6 prefix.	ipv6-prefix	Not Specified	::/0
summary-only	Enable/disable filter more specific routes from updates.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config neighbor

Parameter	Description	Type	Size	Default
activate	Enable/disable address family IPv4 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate-evpn	Enable/disable address family L2VPN EVPN for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate-vpnv4	Enable/disable address family VPNv4 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate-vpnv6	Enable/disable address family VPNv6 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate6	Enable/disable address family IPv6 for this neighbor.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
additional-path	Enable/disable IPv4 additional-path capability.	option	-	disable
	Option	Description		
	<i>send</i>	Enable sending additional paths.		
	<i>receive</i>	Enable receiving additional paths.		
	<i>both</i>	Enable sending and receiving additional paths.		
	<i>disable</i>	Disable additional paths.		
additional-path-vpnv4	Enable/disable VPNv4 additional-path capability.	option	-	disable
	Option	Description		
	<i>send</i>	Enable sending additional paths.		
	<i>receive</i>	Enable receiving additional paths.		
	<i>both</i>	Enable sending and receiving additional paths.		
	<i>disable</i>	Disable additional paths.		
additional-path-vpnv6	Enable/disable VPNv6 additional-path capability.	option	-	disable
	Option	Description		
	<i>send</i>	Enable sending additional paths.		
	<i>receive</i>	Enable receiving additional paths.		
	<i>both</i>	Enable sending and receiving additional paths.		
	<i>disable</i>	Disable additional paths.		
additional-path6	Enable/disable IPv6 additional-path capability.	option	-	disable
	Option	Description		
	<i>send</i>	Enable sending additional paths.		
	<i>receive</i>	Enable receiving additional paths.		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
	Option	Description								
	<i>both</i>	Enable sending and receiving additional paths.								
<i>disable</i>	Disable additional paths.									
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 2 Maximum value: 255							
adv-additional-path-vpnv4	Number of VPNv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 2 Maximum value: 255							
adv-additional-path-vpnv6	Number of VPNv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 2 Maximum value: 255							
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 2 Maximum value: 255							
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 30 0 Maximum value: 600							
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 3 1 Maximum value: 10							
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
allowas-in-enable-evpn	Enable/disable to allow my AS in AS path for L2VPN EVPN route.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
allowas-in-enable-vpnv4	Enable/disable to allow my AS in AS path for VPNv4 route.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
allowas-in-enable-vpnv6	Enable/disable use of my AS in AS path for VPNv6 route.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
allowas-in-evpn	The maximum number of occurrence of my AS number allowed for L2VPN EVPN route.	integer	Minimum value: 1 Maximum value: 10	3
allowas-in-vpnv4	The maximum number of occurrence of my AS number allowed for VPNv4 route.	integer	Minimum value: 1 Maximum value: 10	3
allowas-in-vpnv6	The maximum number of occurrence of my AS number allowed for VPNv6 route.	integer	Minimum value: 1 Maximum value: 10	3
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	3
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-	
	Option Description			
	<i>as-path</i>	AS path.		
	<i>med</i>	MED.		
	<i>next-hop</i>	Next hop.		
attribute-unchanged-vpnv4	List of attributes that should be unchanged for VPNv4 route.	option	-	
	Option Description			
	<i>as-path</i>	AS path.		
	<i>med</i>	MED.		
	<i>next-hop</i>	Next hop.		
attribute-unchanged-vpnv6	List of attributes that should not be changed for VPNv6 route.	option	-	
	Option Description			
	<i>as-path</i>	AS path.		
	<i>med</i>	MED.		
	<i>next-hop</i>	Next hop.		
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-	
	Option Description			
	<i>as-path</i>	AS path.		
	<i>med</i>	MED.		
	<i>next-hop</i>	Next hop.		
auth-options	Key-chain name for TCP authentication options.	string	Maximum length: 35	
bfd	Enable/disable BFD for this neighbor.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-graceful-restart-evpn	Enable/disable advertisement of L2VPN EVPN graceful restart capability to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default										
capability-graceful-restart-vpnv4	Enable/disable advertise VPNv4 graceful restart capability to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-graceful-restart-vpnv6	Enable/disable advertisement of VPNv6 graceful restart capability to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.							
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
	Option	Description								
	<i>send</i>	Send ORF list.								
<i>both</i>	Send and receive ORF lists.									
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 1 Maximum value: 65535	4294967295						
default-originate-routemap	Route map to specify criteria to originate IPv4 default.	string	Maximum length: 35							
default-originate-routemap6	Route map to specify criteria to originate IPv6 default.	string	Maximum length: 35							
description	Description.	string	Maximum length: 63							
distribute-list-in	Filter for IPv4 updates from this neighbor.	string	Maximum length: 35							
distribute-list-in-vpnv4	Filter for VPNv4 updates from this neighbor.	string	Maximum length: 35							
distribute-list-in-vpnv6	Filter for VPNv6 updates from this neighbor.	string	Maximum length: 35							
distribute-list-in6	Filter for IPv6 updates from this neighbor.	string	Maximum length: 35							
distribute-list-out	Filter for IPv4 updates to this neighbor.	string	Maximum length: 35							
distribute-list-out-vpnv4	Filter for VPNv4 updates to this neighbor.	string	Maximum length: 35							
distribute-list-out-vpnv6	Filter for VPNv6 updates to this neighbor.	string	Maximum length: 35							
distribute-list-out6	Filter for IPv6 updates to this neighbor.	string	Maximum length: 35							
dont-capability-negotiate	Do not negotiate capabilities with this neighbor.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGp neighbors.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 255	255						
filter-list-in	BGP filter for IPv4 inbound routes.	string	Maximum length: 35							
filter-list-in-vpnv4	BGP filter for VPNv4 inbound routes.	string	Maximum length: 35							
filter-list-in-vpnv6	BGP filter for VPNv6 inbound routes.	string	Maximum length: 35							
filter-list-in6	BGP filter for IPv6 inbound routes.	string	Maximum length: 35							
filter-list-out	BGP filter for IPv4 outbound routes.	string	Maximum length: 35							
filter-list-out-vpnv4	BGP filter for VPNv4 outbound routes.	string	Maximum length: 35							
filter-list-out-vpnv6	BGP filter for VPNv6 outbound routes.	string	Maximum length: 35							
filter-list-out6	BGP filter for IPv6 outbound routes.	string	Maximum length: 35							
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535	4294967295						
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15							

Parameter	Description	Type	Size	Default						
ip	IP/IPv6 address of neighbor.	string	Maximum length: 45							
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535	4294967295						
link-down-failover	Enable/disable failover upon link down.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
local-as	Local AS number of neighbor.	user	Not Specified							
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 0 1 Maximum value: 4294967295							
maximum-prefix-evpn	Maximum number of L2VPN EVPN prefixes to accept from this peer.	integer	Minimum value: 0 1 Maximum value: 4294967295							
maximum-prefix-threshold	Maximum IPv4 prefix threshold value (1 - 100 percent).	integer	Minimum value: 1 Maximum value: 100	75						
maximum-prefix-threshold-evpn	Maximum L2VPN EVPN prefix threshold value (1 - 100 percent).	integer	Minimum value: 1 Maximum value: 100	75						

Parameter	Description	Type	Size	Default						
maximum-prefix-threshold-vpnv4	Maximum VPNv4 prefix threshold value (1 - 100 percent).	integer	Minimum value: 1 Maximum value: 100	75						
maximum-prefix-threshold-vpnv6	Maximum VPNv6 prefix threshold value (1 - 100 percent).	integer	Minimum value: 1 Maximum value: 100	75						
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value (1 - 100 percent).	integer	Minimum value: 1 Maximum value: 100	75						
maximum-prefix-vpnv4	Maximum number of VPNv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0						
maximum-prefix-vpnv6	Maximum number of VPNv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0						
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
maximum-prefix-warning-only-evpn	Enable/disable only sending warning message when exceeding limit of L2VPN EVPN routes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
maximum-prefix-warning-only-vpnv4	Enable/disable only giving warning message when limit is exceeded for VPNv4 routes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
maximum-prefix-warning-only-vpnv6	Enable/disable warning message when limit is exceeded for VPNv6 routes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 0 1 Maximum value: 4294967295							
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-rr	Enable/disable setting nexthop's address to interface's IPv4 address for route-reflector routes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-rr6	Enable/disable setting nexthop's address to interface's IPv6 address for route-reflector routes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
next-hop-self-vpnv4	Enable/disable setting VPNv4 next-hop to interface's IP address for this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-vpnv6	Enable/disable use of outgoing interface's IP address as VPNv6 next-hop for this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
override-capability	Enable/disable override result of capability negotiation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
passive	Enable/disable sending of open messages to this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
password	Password used in MD5 authentication.	password	Not Specified							
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
prefix-list-in-vpnv4	Inbound filter for VPNv4 updates from this neighbor.	string	Maximum length: 35	
prefix-list-in-vpnv6	Inbound filter for VPNv6 updates from this neighbor.	string	Maximum length: 35	
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
prefix-list-out-vpnv4	Outbound filter for VPNv4 updates to this neighbor.	string	Maximum length: 35	
prefix-list-out-vpnv6	Outbound filter for VPNv6 updates to this neighbor.	string	Maximum length: 35	
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
remote-as	AS number of neighbor.	user	Not Specified	
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
remove-private-as-evpn	Enable/disable removing private AS number from L2VPN EVPN outbound updates.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
remove-private-as-vpnv4	Enable/disable remove private AS number from VPNv4 outbound updates.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	

Parameter	Description	Type	Size	Default						
remove-private-as-vpnv6	Enable/disable to remove private AS number from VPNv6 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
restart-time	Graceful restart delay time (sec, 0 = global default).	integer	Minimum value: 0 Maximum value: 3600							
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535							
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35							
route-map-in-evpn	L2VPN EVPN inbound route map filter.	string	Maximum length: 35							
route-map-in-vpnv4	VPNv4 inbound route map filter.	string	Maximum length: 35							
route-map-in-vpnv6	VPNv6 inbound route map filter.	string	Maximum length: 35							
route-map-in6	IPv6 Inbound route map filter.	string	Maximum length: 35							
route-map-out	IPv4 outbound route map filter.	string	Maximum length: 35							
route-map-out-evpn	L2VPN EVPN outbound route map filter.	string	Maximum length: 35							
route-map-out-preferable	IPv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35							
route-map-out-vpnv4	VPNv4 outbound route map filter.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
route-map-out-vpnv4-preferable	VPNv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35	
route-map-out-vpnv6	VPNv6 outbound route map filter.	string	Maximum length: 35	
route-map-out-vpnv6-preferable	VPNv6 outbound route map filter if this neighbor is preferred.	string	Maximum length: 35	
route-map-out6	IPv6 Outbound route map filter.	string	Maximum length: 35	
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35	
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-reflector-client-evpn	Enable/disable L2VPN EVPN AS route reflector client for this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-reflector-client-vpnv4	Enable/disable VPNv4 AS route reflector client for this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-reflector-client-vpnv6	Enable/disable VPNv6 AS route reflector client for this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client	Enable/disable IPv4 AS route server client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client-evpn	Enable/disable L2VPN EVPN AS route server client for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client-vpnv4	Enable/disable VPNv4 AS route server client for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client-vpnv6	Enable/disable VPNv6 AS route server client for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client6	Enable/disable IPv6 AS route server client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
rr-attr-allow-change	Enable/disable allowing change of route attributes when advertising to IPv4 route reflector clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
rr-attr-allow-change-evpn	Enable/disable allowing change of route attributes when advertising to L2VPN EVPN route reflector clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
rr-attr-allow-change-vpnv4	Enable/disable allowing change of route attributes when advertising to VPNv4 route reflector clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
rr-attr-allow-change-vpnv6	Enable/disable allowing change of route attributes when advertising to VPNv6 route reflector clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
rr-attr-allow-change6	Enable/disable allowing change of route attributes when advertising to IPv6 route reflector clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
send-community	IPv4 Send community attribute to neighbor.	option	-	both						

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard.</td></tr><tr><td><i>extended</i></td><td>Extended.</td></tr><tr><td><i>both</i></td><td>Both.</td></tr><tr><td><i>disable</i></td><td>Disable</td></tr></table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
	Option	Description												
	<i>standard</i>	Standard.												
	<i>extended</i>	Extended.												
	<i>both</i>	Both.												
	<i>disable</i>	Disable												
send-community-evpn	Enable/disable sending community attribute to neighbor for L2VPN EVPN address family.	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard.</td></tr><tr><td><i>extended</i></td><td>Extended.</td></tr><tr><td><i>both</i></td><td>Both.</td></tr><tr><td><i>disable</i></td><td>Disable</td></tr></table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
	Option	Description												
	<i>standard</i>	Standard.												
	<i>extended</i>	Extended.												
	<i>both</i>	Both.												
	<i>disable</i>	Disable												
send-community-vpnv4	Send community attribute to neighbor for VPNv4 address family.	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard.</td></tr><tr><td><i>extended</i></td><td>Extended.</td></tr><tr><td><i>both</i></td><td>Both.</td></tr><tr><td><i>disable</i></td><td>Disable</td></tr></table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
	Option	Description												
	<i>standard</i>	Standard.												
	<i>extended</i>	Extended.												
	<i>both</i>	Both.												
	<i>disable</i>	Disable												
send-community-vpnv6	Enable/disable sending community attribute to this neighbor for VPNv6 address family.	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard.</td></tr><tr><td><i>extended</i></td><td>Extended.</td></tr><tr><td><i>both</i></td><td>Both.</td></tr><tr><td><i>disable</i></td><td>Disable</td></tr></table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
	Option	Description												
	<i>standard</i>	Standard.												
	<i>extended</i>	Extended.												
	<i>both</i>	Both.												
	<i>disable</i>	Disable												
send-community6	IPv6 Send community attribute to neighbor.	option	-	both										

Parameter	Description	Type	Size	Default
	Option Description			
	<i>standard</i>	Standard.		
	<i>extended</i>	Extended.		
	<i>both</i>	Both.		
	<i>disable</i>	Disable		
shutdown	Enable/disable shutdown this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
soft-reconfiguration-evpn	Enable/disable L2VPN EVPN inbound soft reconfiguration.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
soft-reconfiguration-vpnv4	Enable/disable allow VPNv4 inbound soft reconfiguration.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
soft-reconfiguration-vpnv6	Enable/disable VPNv6 inbound soft reconfiguration.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
stale-route	Enable/disable stale route after neighbor down.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
strict-capability-match	Enable/disable strict capability matching.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35	
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35	
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15	
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535	4294967295

config conditional-advertise

Parameter	Description	Type	Size	Default
advertise-routemap	Name of advertising route map.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
condition-routemap <name>	List of conditional route maps. Route map.	string	Maximum length: 79	
condition-type	Type of condition.	option	-	exist
	Option	Description		
	<i>exist</i>	True if condition route map is matched.		
	<i>non-exist</i>	True if condition route map is not matched.		

config conditional-advertise6

Parameter	Description	Type	Size	Default
advertise-routemap	Name of advertising route map.	string	Maximum length: 35	
condition-routemap <name>	List of conditional route maps. Route map.	string	Maximum length: 79	
condition-type	Type of condition.	option	-	exist
	Option	Description		
	<i>exist</i>	True if condition route map is matched.		
	<i>non-exist</i>	True if condition route map is not matched.		

config neighbor-group

Parameter	Description	Type	Size	Default
activate	Enable/disable address family IPv4 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate-evpn	Enable/disable address family L2VPN EVPN for this neighbor.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate-vpnv4	Enable/disable address family VPNv4 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate-vpnv6	Enable/disable address family VPNv6 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate6	Enable/disable address family IPv6 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
additional-path	Enable/disable IPv4 additional-path capability.	option	-	disable
	Option	Description		
	<i>send</i>	Enable sending additional paths.		
	<i>receive</i>	Enable receiving additional paths.		
	<i>both</i>	Enable sending and receiving additional paths.		
	<i>disable</i>	Disable additional paths.		
additional-path-vpnv4	Enable/disable VPNv4 additional-path capability.	option	-	disable
	Option	Description		
	<i>send</i>	Enable sending additional paths.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>receive</i></td><td>Enable receiving additional paths.</td></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.					
	Option	Description												
	<i>receive</i>	Enable receiving additional paths.												
	<i>both</i>	Enable sending and receiving additional paths.												
	<i>disable</i>	Disable additional paths.												
additional-path-vpnv6	Enable/disable VPNv6 additional-path capability.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>send</i></td><td>Enable sending additional paths.</td></tr><tr><td><i>receive</i></td><td>Enable receiving additional paths.</td></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
	Option	Description												
	<i>send</i>	Enable sending additional paths.												
	<i>receive</i>	Enable receiving additional paths.												
	<i>both</i>	Enable sending and receiving additional paths.												
<i>disable</i>	Disable additional paths.													
additional-path6	Enable/disable IPv6 additional-path capability.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>send</i></td><td>Enable sending additional paths.</td></tr><tr><td><i>receive</i></td><td>Enable receiving additional paths.</td></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
	Option	Description												
	<i>send</i>	Enable sending additional paths.												
	<i>receive</i>	Enable receiving additional paths.												
	<i>both</i>	Enable sending and receiving additional paths.												
<i>disable</i>	Disable additional paths.													
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 2 Maximum value: 255	2										
adv-additional-path-vpnv4	Number of VPNv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 2 Maximum value: 255	2										
adv-additional-path-vpnv6	Number of VPNv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 2 Maximum value: 255	2										
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 2 Maximum value: 255	2										
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 30 0 Maximum value: 600	30										

Parameter	Description	Type	Size	Default						
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	3						
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allowas-in-enable-evpn	Enable/disable to allow my AS in AS path for L2VPN EVPN route.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allowas-in-enable-vpnv4	Enable/disable to allow my AS in AS path for VPNv4 route.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allowas-in-enable-vpnv6	Enable/disable use of my AS in AS path for VPNv6 route.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allowas-in-evpn	The maximum number of occurrence of my AS number allowed for L2VPN EVPN route.	integer	Minimum value: 1 Maximum value: 10	3						

Parameter	Description	Type	Size	Default								
allowas-in-vpnv4	The maximum number of occurrence of my AS number allowed for VPNv4 route.	integer	Minimum value: 1 Maximum value: 10	3								
allowas-in-vpnv6	The maximum number of occurrence of my AS number allowed for VPNv6 route.	integer	Minimum value: 1 Maximum value: 10	3								
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	3								
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
attribute-unchanged-vpnv4	List of attributes that should be unchanged for VPNv4 route.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											

Parameter	Description	Type	Size	Default								
attribute-unchanged-vpnv6	List of attributes that should not be changed for VPNv6 route.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
auth-options	Key-chain name for TCP authentication options.	string	Maximum length: 35									
bfd	Enable/disable BFD for this neighbor.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-graceful-restart-evpn	Enable/disable advertisement of L2VPN EVPN graceful restart capability to this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-graceful-restart-vpnv4	Enable/disable advertise VPNv4 graceful restart capability to this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-graceful-restart-vpnv6	Enable/disable advertisement of VPNv6 graceful restart capability to this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-	disable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
	Option	Description												
	<i>none</i>	None.												
	<i>receive</i>	Receive ORF lists.												
	<i>send</i>	Send ORF list.												
<i>both</i>	Send and receive ORF lists.													
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
	Option	Description												
	<i>none</i>	None.												
	<i>receive</i>	Receive ORF lists.												
	<i>send</i>	Send ORF list.												
<i>both</i>	Send and receive ORF lists.													
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 1 Maximum value: 65535	4294967295										
default-originate-routemap	Route map to specify criteria to originate IPv4 default.	string	Maximum length: 35											
default-originate-routemap6	Route map to specify criteria to originate IPv6 default.	string	Maximum length: 35											
description	Description.	string	Maximum length: 63											

Parameter	Description	Type	Size	Default						
distribute-list-in	Filter for IPv4 updates from this neighbor.	string	Maximum length: 35							
distribute-list-in-vpnv4	Filter for VPNv4 updates from this neighbor.	string	Maximum length: 35							
distribute-list-in-vpnv6	Filter for VPNv6 updates from this neighbor.	string	Maximum length: 35							
distribute-list-in6	Filter for IPv6 updates from this neighbor.	string	Maximum length: 35							
distribute-list-out	Filter for IPv4 updates to this neighbor.	string	Maximum length: 35							
distribute-list-out-vpnv4	Filter for VPNv4 updates to this neighbor.	string	Maximum length: 35							
distribute-list-out-vpnv6	Filter for VPNv6 updates to this neighbor.	string	Maximum length: 35							
distribute-list-out6	Filter for IPv6 updates to this neighbor.	string	Maximum length: 35							
dont-capability-negotiate	Do not negotiate capabilities with this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
ebgp-enforce-multihop	Enable/disable allow multi-hop EGBP neighbors.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 255 1 Maximum value: 255							
filter-list-in	BGP filter for IPv4 inbound routes.	string	Maximum length: 35							
filter-list-in-vpnv4	BGP filter for VPNv4 inbound routes.	string	Maximum length: 35							
filter-list-in-vpnv6	BGP filter for VPNv6 inbound routes.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
filter-list-in6	BGP filter for IPv6 inbound routes.	string	Maximum length: 35							
filter-list-out	BGP filter for IPv4 outbound routes.	string	Maximum length: 35							
filter-list-out-vpnv4	BGP filter for VPNv4 outbound routes.	string	Maximum length: 35							
filter-list-out-vpnv6	BGP filter for VPNv6 outbound routes.	string	Maximum length: 35							
filter-list-out6	BGP filter for IPv6 outbound routes.	string	Maximum length: 35							
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535	4294967295						
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15							
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535	4294967295						
link-down-failover	Enable/disable failover upon link down.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
local-as	Local AS number of neighbor.	user	Not Specified							
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 0 1 Maximum value: 4294967295							
maximum-prefix-evpn	Maximum number of L2VPN EVPN prefixes to accept from this peer.	integer	Minimum value: 0 1 Maximum value: 4294967295							
maximum-prefix-threshold	Maximum IPv4 prefix threshold value (1 - 100 percent).	integer	Minimum value: 75 1 Maximum value: 100							
maximum-prefix-threshold-evpn	Maximum L2VPN EVPN prefix threshold value (1 - 100 percent).	integer	Minimum value: 75 1 Maximum value: 100							
maximum-prefix-threshold-vpnv4	Maximum VPNv4 prefix threshold value (1 - 100 percent).	integer	Minimum value: 75 1 Maximum value: 100							
maximum-prefix-threshold-vpnv6	Maximum VPNv6 prefix threshold value (1 - 100 percent).	integer	Minimum value: 75 1 Maximum value: 100							
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value (1 - 100 percent).	integer	Minimum value: 75 1 Maximum value: 100							
maximum-prefix-vpnv4	Maximum number of VPNv4 prefixes to accept from this peer.	integer	Minimum value: 0 1 Maximum value: 4294967295							
maximum-prefix-vpnv6	Maximum number of VPNv6 prefixes to accept from this peer.	integer	Minimum value: 0 1 Maximum value: 4294967295							
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
maximum-prefix-warning-only-evpn	Enable/disable only sending warning message when exceeding limit of L2VPN EVPN routes.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
maximum-prefix-warning-only-vpnv4	Enable/disable only giving warning message when limit is exceeded for VPNv4 routes.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
maximum-prefix-warning-only-vpnv6	Enable/disable warning message when limit is exceeded for VPNv6 routes.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 0 1 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default						
name	Neighbor group name.	string	Maximum length: 45							
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-rr	Enable/disable setting nexthop's address to interface's IPv4 address for route-reflector routes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-rr6	Enable/disable setting nexthop's address to interface's IPv6 address for route-reflector routes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-vpnv4	Enable/disable setting VPNv4 next-hop to interface's IP address for this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
next-hop-self-vpnv6	Enable/disable use of outgoing interface's IP address as VPNv6 next-hop for this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
override-capability	Enable/disable override result of capability negotiation.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
passive	Enable/disable sending of open messages to this neighbor.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
password	Password used in MD5 authentication.	password	Not Specified	
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-in-vpnv4	Inbound filter for VPNv4 updates from this neighbor.	string	Maximum length: 35	
prefix-list-in-vpnv6	Inbound filter for VPNv6 updates from this neighbor.	string	Maximum length: 35	
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
prefix-list-out-vpnv4	Outbound filter for VPNv4 updates to this neighbor.	string	Maximum length: 35	
prefix-list-out-vpnv6	Outbound filter for VPNv6 updates to this neighbor.	string	Maximum length: 35	
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
remote-as	AS number of neighbor.	user	Not Specified	

Parameter	Description	Type	Size	Default						
remote-as-filter	BGP filter for remote AS.	string	Maximum length: 35							
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as-evpn	Enable/disable removing private AS number from L2VPN EVPN outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as-vpnv4	Enable/disable remove private AS number from VPNv4 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as-vpnv6	Enable/disable to remove private AS number from VPNv6 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
restart-time	Graceful restart delay time (sec, 0 = global default).	integer	Minimum value: 0 Maximum value: 3600	0
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535	0
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35	
route-map-in-evpn	L2VPN EVPN inbound route map filter.	string	Maximum length: 35	
route-map-in-vpnv4	VPNv4 inbound route map filter.	string	Maximum length: 35	
route-map-in-vpnv6	VPNv6 inbound route map filter.	string	Maximum length: 35	
route-map-in6	IPv6 Inbound route map filter.	string	Maximum length: 35	
route-map-out	IPv4 outbound route map filter.	string	Maximum length: 35	
route-map-out-evpn	L2VPN EVPN outbound route map filter.	string	Maximum length: 35	
route-map-out-preferable	IPv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35	
route-map-out-vpnv4	VPNv4 outbound route map filter.	string	Maximum length: 35	
route-map-out-vpnv4-preferable	VPNv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35	
route-map-out-vpnv6	VPNv6 outbound route map filter.	string	Maximum length: 35	
route-map-out-vpnv6-preferable	VPNv6 outbound route map filter if this neighbor is preferred.	string	Maximum length: 35	
route-map-out6	IPv6 Outbound route map filter.	string	Maximum length: 35	
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35	
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-reflector-client-evpn	Enable/disable L2VPN EVPN AS route reflector client for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-reflector-client-vpnv4	Enable/disable VPNv4 AS route reflector client for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-reflector-client-vpnv6	Enable/disable VPNv6 AS route reflector client for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client	Enable/disable IPv4 AS route server client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client-evpn	Enable/disable L2VPN EVPN AS route server client for this neighbor.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client-vpnv4	Enable/disable VPNv4 AS route server client for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client-vpnv6	Enable/disable VPNv6 AS route server client for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client6	Enable/disable IPv6 AS route server client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
rr-attr-allow-change	Enable/disable allowing change of route attributes when advertising to IPv4 route reflector clients.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
rr-attr-allow-change-evpn	Enable/disable allowing change of route attributes when advertising to L2VPN EVPN route reflector clients.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
rr-attr-allow-change-vpnv4	Enable/disable allowing change of route attributes when advertising to VPNv4 route reflector clients.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
rr-attr-allow-change-vpnv6	Enable/disable allowing change of route attributes when advertising to VPNv6 route reflector clients.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
rr-attr-allow-change6	Enable/disable allowing change of route attributes when advertising to IPv6 route reflector clients.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
send-community	IPv4 Send community attribute to neighbor.	option	-	both
	Option	Description		
	<i>standard</i>	Standard.		
	<i>extended</i>	Extended.		
	<i>both</i>	Both.		
send-community-evpn	Enable/disable sending community attribute to neighbor for L2VPN EVPN address family.	option	-	both
	Option	Description		
	<i>standard</i>	Standard.		
	<i>extended</i>	Extended.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>both</i>	Both.		
	<i>disable</i>	Disable		
send-community-vpnv4	Send community attribute to neighbor for VPNv4 address family.	option	-	both
	Option	Description		
	<i>standard</i>	Standard.		
	<i>extended</i>	Extended.		
	<i>both</i>	Both.		
	<i>disable</i>	Disable		
send-community-vpnv6	Enable/disable sending community attribute to this neighbor for VPNv6 address family.	option	-	both
	Option	Description		
	<i>standard</i>	Standard.		
	<i>extended</i>	Extended.		
	<i>both</i>	Both.		
	<i>disable</i>	Disable		
send-community6	IPv6 Send community attribute to neighbor.	option	-	both
	Option	Description		
	<i>standard</i>	Standard.		
	<i>extended</i>	Extended.		
	<i>both</i>	Both.		
	<i>disable</i>	Disable		
shutdown	Enable/disable shutdown this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration-evpn	Enable/disable L2VPN EVPN inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration-vpnv4	Enable/disable allow VPNv4 inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration-vpnv6	Enable/disable VPNv6 inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
stale-route	Enable/disable stale route after neighbor down.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
strict-capability-match	Enable/disable strict capability matching.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35							
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35							
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15							
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535	4294967295						

config neighbor-range

Parameter	Description	Type	Size	Default
id	Neighbor range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000	0
neighbor-group	Neighbor group name.	string	Maximum length: 63	
prefix	Neighbor range prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config neighbor-range6

Parameter	Description	Type	Size	Default
id	IPv6 neighbor range ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 1 Maximum value: 1000	0
neighbor-group	Neighbor group name.	string	Maximum length: 63	
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0

config network

Parameter	Description	Type	Size	Default
backdoor	Enable/disable route as backdoor.	option	-	disable
	Option Description			
	enable	Enable setting.		
	disable	Disable setting.		
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
network-import-check	Configure insurance of BGP network route existence in IGP.	option	-	global
	Option Description			
	global	Use global network sync value.		
	enable	Enable network sync per prefix.		
	disable	Disable network sync per prefix.		
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
prefix-name	Name of firewall address or address group.	string	Maximum length: 79	
route-map	Route map to modify generated route.	string	Maximum length: 35	

config network6

Parameter	Description	Type	Size	Default
backdoor	Enable/disable route as backdoor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
network-import-check	Configure insurance of BGP network route existence in IGP.	option	-	global
	Option	Description		
	<i>global</i>	Use global network sync value.		
	<i>enable</i>	Enable network sync per prefix.		
	<i>disable</i>	Disable network sync per prefix.		
prefix6	Network IPv6 prefix.	ipv6-network	Not Specified	::/0
route-map	Route map to modify generated route.	string	Maximum length: 35	

config redistribute

Parameter	Description	Type	Size	Default
name	Distribute list entry name.	string	Maximum length: 35	
route-map	Route map name.	string	Maximum length: 35	
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config redistribute6

Parameter	Description	Type	Size	Default
name	Distribute list entry name.	string	Maximum length: 35	
route-map	Route map name.	string	Maximum length: 35	
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config vrf

Parameter	Description	Type	Size	Default
export-rt <route-target>	List of export route target. Attribute: AA:NN A.B.C.D:NN.	string	Maximum length: 79	
import-route-map	Import route map.	string	Maximum length: 35	
import-rt <route-target>	List of import route target. Attribute: AA:NN A.B.C.D:NN	string	Maximum length: 79	
rd	Route Distinguisher: AA:NN A.B.C.D:NN.	string	Maximum length: 79	
role	VRF role.	option	-	standalone
	Option	Description		
	<i>standalone</i>	Stand-alone VRF.		
	<i>ce</i>	CE VRF.		
	<i>pe</i>	PE VRF.		
vrf	Origin VRF ID <0-511>.	string	Maximum length: 7	

config leak-target

Parameter	Description	Type	Size	Default
interface	Interface which is used to leak routes to target VRF.	string	Maximum length: 15	
route-map	Route map of VRF leaking.	string	Maximum length: 35	
vrf	Target VRF ID <0-511>.	string	Maximum length: 7	

config vrf6

Parameter	Description	Type	Size	Default								
export-rt <route-target>	List of export route target. Attribute: AA:NN A.B.C.D:NN.	string	Maximum length: 79									
import-route-map	Import route map.	string	Maximum length: 35									
import-rt <route-target>	List of import route target. Attribute: AA:NN A.B.C.D:NN	string	Maximum length: 79									
rd	Route Distinguisher: AA:NN A.B.C.D:NN.	string	Maximum length: 79									
role	VRF role.	option	-	standalone								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>standalone</td><td>Stand-alone VRF.</td></tr><tr><td>ce</td><td>CE VRF.</td></tr><tr><td>pe</td><td>PE VRF.</td></tr></table>	Option	Description	standalone	Stand-alone VRF.	ce	CE VRF.	pe	PE VRF.			
Option	Description											
standalone	Stand-alone VRF.											
ce	CE VRF.											
pe	PE VRF.											
vrf	Origin VRF ID <0-511>.	string	Maximum length: 7									

config leak-target

Parameter	Description	Type	Size	Default
interface	Interface which is used to leak routes to target VRF.	string	Maximum length: 15	
route-map	Route map of VRF leaking.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
vrf	Target VRF ID <0-511>.	string	Maximum length: 7	

config router community-list

Configure community lists.

```

config router community-list
  Description: Configure community lists.
  edit <name>
    config rule
      Description: Community list rule.
      edit <id>
        set action [deny|permit]
        set match {string}
        set regexp {string}
      next
    end
    set type [standard|expanded]
  next
end

```

config router community-list

Parameter	Description	Type	Size	Default						
name	Community list name.	string	Maximum length: 35							
type	Community list type (standard or expanded).	option	-	standard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard community list type.</td></tr><tr><td><i>expanded</i></td><td>Expanded community list type.</td></tr></table>				Option	Description	<i>standard</i>	Standard community list type.	<i>expanded</i>	Expanded community list type.
	Option	Description								
	<i>standard</i>	Standard community list type.								
<i>expanded</i>	Expanded community list type.									

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny route-based operations, based on the route's COMMUNITY attribute.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>deny</i>	Deny route-based operations.		
	<i>permit</i>	Permit or allow route-based operations.		
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
match	Community specifications for matching a reserved community.	string	Maximum length: 255	
regex	Ordered list of COMMUNITY attributes as a regular expression.	string	Maximum length: 255	

config router extcommunity-list

Configure extended community lists.

```

config router extcommunity-list
  Description: Configure extended community lists.
  edit <name>
    config rule
      Description: Extended community list rule.
      edit <id>
        set action [deny|permit]
        set match {string}
        set regex {string}
        set type [rt|soo]
      next
    end
    set type [standard|expanded]
  next
end

```

config router extcommunity-list

Parameter	Description	Type	Size	Default
name	Extended community list name.	string	Maximum length: 35	
type	Extended community list type (standard or expanded).	option	-	standard

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>standard</i>	Standard extended community list type.		
	<i>expanded</i>	Expanded extended community list type.		

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny route-based operations, based on the route's EXTENDED COMMUNITY attribute.	option	-	
	Option	Description		
	<i>deny</i>	Deny route-based operations.		
	<i>permit</i>	Permit or allow route-based operations.		
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
match	Extended community specifications for matching a reserved extended community.	string	Maximum length: 255	
regex	Ordered list of EXTENDED COMMUNITY attributes as a regular expression.	string	Maximum length: 255	
type	Type of extended community.	option	-	rt
	Option	Description		
	<i>rt</i>	Route Target.		
	<i>soo</i>	Site of Origin.		

config router isis

Configure IS-IS.

```
config router isis
  Description: Configure IS-IS.
  set adjacency-check [enable|disable]
  set adjacency-check6 [enable|disable]
  set adv-passive-only [enable|disable]
  set adv-passive-only6 [enable|disable]
```



```

set auth-keychain-11 {string}
set auth-keychain-12 {string}
set auth-mode-11 [password|md5]
set auth-mode-12 [password|md5]
set auth-password-11 {password}
set auth-password-12 {password}
set auth-sendonly-11 [enable|disable]
set auth-sendonly-12 [enable|disable]
set default-originate [enable|disable]
set default-originate6 [enable|disable]
set dynamic-hostname [enable|disable]
set ignore-lsp-errors [enable|disable]
set is-type [level-1-2|level-1|...]
config isis-interface
    Description: IS-IS interface configuration.
    edit <name>
        set auth-keychain-11 {string}
        set auth-keychain-12 {string}
        set auth-mode-11 [md5|password]
        set auth-mode-12 [md5|password]
        set auth-password-11 {password}
        set auth-password-12 {password}
        set auth-send-only-11 [enable|disable]
        set auth-send-only-12 [enable|disable]
        set circuit-type [level-1-2|level-1|...]
        set csnp-interval-11 {integer}
        set csnp-interval-12 {integer}
        set hello-interval-11 {integer}
        set hello-interval-12 {integer}
        set hello-multiplier-11 {integer}
        set hello-multiplier-12 {integer}
        set hello-padding [enable|disable]
        set lsp-interval {integer}
        set lsp-retransmit-interval {integer}
        set mesh-group [enable|disable]
        set mesh-group-id {integer}
        set metric-11 {integer}
        set metric-12 {integer}
        set network-type [broadcast|point-to-point|...]
        set priority-11 {integer}
        set priority-12 {integer}
        set status [enable|disable]
        set status6 [enable|disable]
        set wide-metric-11 {integer}
        set wide-metric-12 {integer}
    next
end
config isis-net
    Description: IS-IS net configuration.
    edit <id>
        set net {user}
    next

```

```

end
set lsp-gen-interval-l1 {integer}
set lsp-gen-interval-l2 {integer}
set lsp-refresh-interval {integer}
set max-lsp-lifetime {integer}
set metric-style [narrow|wide|...]
set overload-bit [enable|disable]
set overload-bit-on-startup {integer}
set overload-bit-suppress {option1}, {option2}, ...
config redistribute
    Description: IS-IS redistribute protocols. Read-only.
    edit <protocol>
        set level [level-1-2|level-1|...]
        set metric {integer}
        set metric-type [external|internal]
        set routemap {string}
        set status [enable|disable]
    next
end
set redistribute-l1 [enable|disable]
set redistribute-l1-list {string}
set redistribute-l2 [enable|disable]
set redistribute-l2-list {string}
config redistribute6
    Description: IS-IS IPv6 redistribution for routing protocols. Read-only.
    edit <protocol>
        set level [level-1-2|level-1|...]
        set metric {integer}
        set metric-type [external|internal]
        set routemap {string}
        set status [enable|disable]
    next
end
set redistribute6-l1 [enable|disable]
set redistribute6-l1-list {string}
set redistribute6-l2 [enable|disable]
set redistribute6-l2-list {string}
set spf-interval-exp-l1 {user}
set spf-interval-exp-l2 {user}
config summary-address
    Description: IS-IS summary addresses.
    edit <id>
        set level [level-1-2|level-1|...]
        set prefix {ipv4-classnet-any}
    next
end
config summary-address6
    Description: IS-IS IPv6 summary address.
    edit <id>
        set level [level-1-2|level-1|...]
        set prefix6 {ipv6-prefix}
    next

```

```
end
end
```

config router isis

Parameter	Description	Type	Size	Default
adjacency-check	Enable/disable adjacency check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable adjacency check.		
	<i>disable</i>	Disable adjacency check.		
adjacency-check6	Enable/disable IPv6 adjacency check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPv6 adjacency check.		
	<i>disable</i>	Disable IPv6 adjacency check.		
adv-passive-only	Enable/disable IS-IS advertisement of passive interfaces only.	option	-	disable
	Option	Description		
	<i>enable</i>	Advertise passive interfaces only.		
	<i>disable</i>	Advertise all IS-IS enabled interfaces.		
adv-passive-only6	Enable/disable IPv6 IS-IS advertisement of passive interfaces only.	option	-	disable
	Option	Description		
	<i>enable</i>	Advertise passive interfaces only.		
	<i>disable</i>	Advertise all IS-IS enabled interfaces.		
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35	
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35	
auth-mode-l1	Level 1 authentication mode.	option	-	password

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>password</i>	Password.		
	<i>md5</i>	MD5.		
auth-mode-l2	Level 2 authentication mode.	option	-	password
	Option	Description		
	<i>password</i>	Password.		
	<i>md5</i>	MD5.		
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified	
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified	
auth-sendonly-l1	Enable/disable level 1 authentication send-only.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable level 1 authentication send-only.		
	<i>disable</i>	Disable level 1 authentication send-only.		
auth-sendonly-l2	Enable/disable level 2 authentication send-only.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable level 2 authentication send-only.		
	<i>disable</i>	Disable level 2 authentication send-only.		
default-originate	Enable/disable distribution of default route information.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable distribution of default route information.		
	<i>disable</i>	Disable distribution of default route information.		
default-originate6	Enable/disable distribution of default IPv6 route information.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable distribution of default IPv6 route information.		
	<i>disable</i>	Disable distribution of default IPv6 route information.		
dynamic-hostname	Enable/disable dynamic hostname.	option	-	disable
	Option Description			
	<i>enable</i>	Enable dynamic hostname.		
	<i>disable</i>	Disable dynamic hostname.		
ignore-lsp-errors	Enable/disable ignoring of LSP errors with bad checksums.	option	-	disable
	Option Description			
	<i>enable</i>	Enable ignoring of LSP errors with bad checksums.		
	<i>disable</i>	Disable ignoring of LSP errors with bad checksums.		
is-type	IS type.	option	-	level-1-2
	Option Description			
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1 only.		
	<i>level-2-only</i>	Level 2 only.		
lsp-gen-interval-l1	Minimum interval for level 1 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120	30
lsp-gen-interval-l2	Minimum interval for level 2 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120	30
lsp-refresh-interval	LSP refresh time in seconds.	integer	Minimum value: 1 Maximum value: 65535	900

Parameter	Description	Type	Size	Default
max-lsp-lifetime	Maximum LSP lifetime in seconds.	integer	Minimum value: 350 Maximum value: 65535	1200
metric-style	Use old-style (ISO 10589) or new-style packet formats.	option	-	narrow
	Option	Description		
	<i>narrow</i>	Use old style of TLVs with narrow metric.		
	<i>wide</i>	Use new style of TLVs to carry wider metric.		
	<i>transition</i>	Send and accept both styles of TLVs during transition.		
	<i>narrow-transition</i>	Narrow and accept both styles of TLVs during transition.		
	<i>narrow-transition-l1</i>	Narrow-transition level-1 only.		
	<i>narrow-transition-l2</i>	Narrow-transition level-2 only.		
	<i>wide-l1</i>	Wide level-1 only.		
	<i>wide-l2</i>	Wide level-2 only.		
	<i>wide-transition</i>	Wide and accept both styles of TLVs during transition.		
	<i>wide-transition-l1</i>	Wide-transition level-1 only.		
	<i>wide-transition-l2</i>	Wide-transition level-2 only.		
	<i>transition-l1</i>	Transition level-1 only.		
	<i>transition-l2</i>	Transition level-2 only.		
overload-bit	Enable/disable signal other routers not to use us in SPF.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable overload bit.		
	<i>disable</i>	Disable overload bit.		

Parameter	Description	Type	Size	Default						
overload-bit-on-startup	Overload-bit only temporarily after reboot.	integer	Minimum value: 5 Maximum value: 86400	0						
overload-bit-suppress	Suppress overload-bit for the specific prefixes.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>external</i></td><td>External.</td></tr><tr><td><i>interlevel</i></td><td>Inter-level.</td></tr></table>	Option	Description	<i>external</i>	External.	<i>interlevel</i>	Inter-level.			
Option	Description									
<i>external</i>	External.									
<i>interlevel</i>	Inter-level.									
redistribute-l1	Enable/disable redistribution of level 1 routes into level 2.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redistribution of level 1 routes into level 2.</td></tr><tr><td><i>disable</i></td><td>Disable redistribution of level 1 routes into level 2.</td></tr></table>	Option	Description	<i>enable</i>	Enable redistribution of level 1 routes into level 2.	<i>disable</i>	Disable redistribution of level 1 routes into level 2.			
Option	Description									
<i>enable</i>	Enable redistribution of level 1 routes into level 2.									
<i>disable</i>	Disable redistribution of level 1 routes into level 2.									
redistribute-l1-list	Access-list for route redistribution from l1 to l2.	string	Maximum length: 35							
redistribute-l2	Enable/disable redistribution of level 2 routes into level 1.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redistribution of level 2 routes into level 1.</td></tr><tr><td><i>disable</i></td><td>Disable redistribution of level 2 routes into level 1.</td></tr></table>	Option	Description	<i>enable</i>	Enable redistribution of level 2 routes into level 1.	<i>disable</i>	Disable redistribution of level 2 routes into level 1.			
Option	Description									
<i>enable</i>	Enable redistribution of level 2 routes into level 1.									
<i>disable</i>	Disable redistribution of level 2 routes into level 1.									
redistribute-l2-list	Access-list for route redistribution from l2 to l1.	string	Maximum length: 35							
redistribute6-l1	Enable/disable redistribution of level 1 IPv6 routes into level 2.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redistribution of level 1 IPv6 routes into level 2.</td></tr><tr><td><i>disable</i></td><td>Disable redistribution of level 1 IPv6 routes into level 2.</td></tr></table>	Option	Description	<i>enable</i>	Enable redistribution of level 1 IPv6 routes into level 2.	<i>disable</i>	Disable redistribution of level 1 IPv6 routes into level 2.			
Option	Description									
<i>enable</i>	Enable redistribution of level 1 IPv6 routes into level 2.									
<i>disable</i>	Disable redistribution of level 1 IPv6 routes into level 2.									
redistribute6-l1-list	Access-list for IPv6 route redistribution from l1 to l2.	string	Maximum length: 35							
redistribute6-l2	Enable/disable redistribution of level 2 IPv6 routes into level 1.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable redistribution of level 2 IPv6 routes into level 1.		
	<i>disable</i>	Disable redistribution of level 2 IPv6 routes into level 1.		
redistribute6-l2-list	Access-list for IPv6 route redistribution from l2 to l1.	string	Maximum length: 35	
spf-interval-exp-l1	Level 1 SPF calculation delay.	user	Not Specified	
spf-interval-exp-l2	Level 2 SPF calculation delay.	user	Not Specified	

config isis-interface

Parameter	Description	Type	Size	Default
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35	
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35	
auth-mode-l1	Level 1 authentication mode.	option	-	password
	Option	Description		
	<i>md5</i>	MD5.		
	<i>password</i>	Password.		
auth-mode-l2	Level 2 authentication mode.	option	-	password
	Option	Description		
	<i>md5</i>	MD5.		
	<i>password</i>	Password.		
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified	
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified	
auth-send-only-l1	Enable/disable authentication send-only for level 1 PDUs.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication send-only for level 1 PDUs.</td></tr><tr><td><i>disable</i></td><td>Disable authentication send-only for level 1 PDUs.</td></tr></table>				Option	Description	<i>enable</i>	Enable authentication send-only for level 1 PDUs.	<i>disable</i>	Disable authentication send-only for level 1 PDUs.		
	Option	Description										
	<i>enable</i>	Enable authentication send-only for level 1 PDUs.										
<i>disable</i>	Disable authentication send-only for level 1 PDUs.											
auth-send-only-l2	Enable/disable authentication send-only for level 2 PDUs.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication send-only for level 2 PDUs.</td></tr><tr><td><i>disable</i></td><td>Disable authentication send-only for level 2 PDUs.</td></tr></table>				Option	Description	<i>enable</i>	Enable authentication send-only for level 2 PDUs.	<i>disable</i>	Disable authentication send-only for level 2 PDUs.		
	Option	Description										
	<i>enable</i>	Enable authentication send-only for level 2 PDUs.										
<i>disable</i>	Disable authentication send-only for level 2 PDUs.											
circuit-type	IS-IS interface's circuit type.	option	-	level-1-2								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>level-1-2</i></td><td>Level 1 and 2.</td></tr><tr><td><i>level-1</i></td><td>Level 1.</td></tr><tr><td><i>level-2</i></td><td>Level 2.</td></tr></table>				Option	Description	<i>level-1-2</i>	Level 1 and 2.	<i>level-1</i>	Level 1.	<i>level-2</i>	Level 2.
	Option	Description										
	<i>level-1-2</i>	Level 1 and 2.										
	<i>level-1</i>	Level 1.										
<i>level-2</i>	Level 2.											
csnp-interval-l1	Level 1 CSNP interval.	integer	Minimum value: 10 1 Maximum value: 65535	10								
csnp-interval-l2	Level 2 CSNP interval.	integer	Minimum value: 10 1 Maximum value: 65535	10								
hello-interval-l1	Level 1 hello interval.	integer	Minimum value: 10 0 Maximum value: 65535	10								
hello-interval-l2	Level 2 hello interval.	integer	Minimum value: 10 0 Maximum value: 65535	10								
hello-multiplier-l1	Level 1 multiplier for Hello holding time.	integer	Minimum value: 3 2 Maximum value: 100	3								
hello-multiplier-l2	Level 2 multiplier for Hello holding time.	integer	Minimum value: 3 2 Maximum value: 100	3								
hello-padding	Enable/disable padding to IS-IS hello packets.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable padding to IS-IS hello packets.		
	<i>disable</i>	Disable padding to IS-IS hello packets.		
lsp-interval	LSP transmission interval (milliseconds).	integer	Minimum value: 33 1 Maximum value: 4294967295	
lsp-retransmit-interval	LSP retransmission interval (sec).	integer	Minimum value: 5 1 Maximum value: 65535	
mesh-group	Enable/disable IS-IS mesh group.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IS-IS mesh group.		
	<i>disable</i>	Disable IS-IS mesh group.		
mesh-group-id	Mesh group ID <0-4294967295>, 0: mesh-group blocked.	integer	Minimum value: 0 0 Maximum value: 4294967295	
metric-l1	Level 1 metric for interface.	integer	Minimum value: 10 1 Maximum value: 63	
metric-l2	Level 2 metric for interface.	integer	Minimum value: 10 1 Maximum value: 63	
name	IS-IS interface name.	string	Maximum length: 15	
network-type	IS-IS interface's network type.	option	-	
	Option	Description		
	<i>broadcast</i>	Broadcast.		
	<i>point-to-point</i>	Point-to-point.		
	<i>loopback</i>	Loopback.		
priority-l1	Level 1 priority.	integer	Minimum value: 64 0 Maximum value: 127	

Parameter	Description	Type	Size	Default
priority-l2	Level 2 priority.	integer	Minimum value: 0 Maximum value: 127	64
status	Enable/disable interface for IS-IS.	option	-	disable
	Option	Description		
	enable	Enable interface for IS-IS.		
	disable	Disable interface for IS-IS.		
status6	Enable/disable IPv6 interface for IS-IS.	option	-	disable
	Option	Description		
	enable	Enable IPv6 interface for IS-IS.		
	disable	Disable IPv6 interface for IS-IS.		
wide-metric-l1	Level 1 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214	10
wide-metric-l2	Level 2 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214	10

config isis-net

Parameter	Description	Type	Size	Default
id	ISIS network ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
net	IS-IS networks (format = xx.xxxx.xxxx.xx.).	user	Not Specified	

config redistribute

Parameter	Description	Type	Size	Default
level	Level.	option	-	level-2
	Option	Description		
	level-1-2	Level 1 and 2.		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864	0
metric-type	Metric type.	option	-	internal
	Option Description			
	<i>external</i>	External.		
	<i>internal</i>	Internal.		
protocol	Protocol name.	string	Maximum length: 35	
route-map	Route map name.	string	Maximum length: 35	
status	Status.	option	-	disable
	Option Description			
	<i>enable</i>	Enable.		
	<i>disable</i>	Disable.		

config redistribute6

Parameter	Description	Type	Size	Default
level	Level.	option	-	level-2
	Option Description			
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		

Parameter	Description	Type	Size	Default						
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864	0						
metric-type	Metric type.	option	-	internal						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>external</i></td><td>External metric type.</td></tr><tr><td><i>internal</i></td><td>Internal metric type.</td></tr></table>				Option	Description	<i>external</i>	External metric type.	<i>internal</i>	Internal metric type.
Option	Description									
<i>external</i>	External metric type.									
<i>internal</i>	Internal metric type.									
protocol	Protocol name.	string	Maximum length: 35							
routemap	Route map name.	string	Maximum length: 35							
status	Enable/disable redistribution.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redistribution.</td></tr><tr><td><i>disable</i></td><td>Disable redistribution.</td></tr></table>				Option	Description	<i>enable</i>	Enable redistribution.	<i>disable</i>	Disable redistribution.
Option	Description									
<i>enable</i>	Enable redistribution.									
<i>disable</i>	Disable redistribution.									

config summary-address

Parameter	Description	Type	Size	Default
id	Summary address entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
level	Level.	option	-	level-2
	OptionDescription			
	level-1-2	Level 1 and 2.		
	level-1	Level 1.		
	level-2	Level 2.		
prefix	Prefix.	ipv4- classnet- any	Not Specified	0.0.0.0 0.0.0.0

config summary-address6

Parameter	Description	Type	Size	Default
id	Prefix entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
level	Level.	option	-	level-2
	Option		Description	
	level-1-2		Level 1 and 2.	
	level-1		Level 1.	
	level-2		Level 2.	
prefix6	IPv6 prefix.	ipv6-prefix	Not Specified	::/0

config router key-chain

Configure key-chain.

```
config router key-chain
  Description: Configure key-chain.
  edit <name>
    config key
      Description: Configuration method to edit key settings.
      edit <id>
        set accept-lifetime {user}
        set algorithm [md5|hmac-sha1|...]
        set key-string {password}
        set send-lifetime {user}
      next
    end
  next
end
```

config router key-chain

Parameter	Description	Type	Size	Default
name	Key-chain name.	string	Maximum length: 35	

config key

Parameter	Description	Type	Size	Default
accept-lifetime	Lifetime of received authentication key (format: hh:mm:ss day month year).	user	Not Specified	
algorithm	Cryptographic algorithm.	option	-	md5
	Option	Description		
	<i>md5</i>	MD5.		
	<i>hmac-sha1</i>	HMAC-SHA1.		
	<i>hmac-sha256</i>	HMAC-SHA256.		
	<i>hmac-sha384</i>	HMAC-SHA384.		
	<i>hmac-sha512</i>	HMAC-SHA512.		
	<i>cmac-aes128</i>	CMAC-AES128.		
id	Key ID (0 - 2147483647).	string	Maximum length: 10	
key-string	Password for the key (maximum = 64 characters).	password	Not Specified	
send-lifetime	Lifetime of sent authentication key (format: hh:mm:ss day month year).	user	Not Specified	

config router multicast

Configure router multicast.

```
config router multicast
  Description: Configure router multicast.
  config interface
    Description: PIM interfaces.
    edit <name>
      set bfd [enable|disable]
      set cisco-exclude-genid [enable|disable]
      set dr-priority {integer}
      set hello-holdtime {integer}
      set hello-interval {integer}
    config igmp
      Description: IGMP configuration options.
      set access-group {string}
      set immediate-leave-group {string}
      set last-member-query-count {integer}
      set last-member-query-interval {integer}
      set query-interval {integer}
```

```

        set query-max-response-time {integer}
        set query-timeout {integer}
        set router-alert-check [enable|disable]
        set version [3|2|...]
    end
    config join-group
        Description: Join multicast groups.
        edit <address>
            next
        end
        set multicast-flow {string}
        set neighbour-filter {string}
        set passive [enable|disable]
        set pim-mode [sparse-mode|dense-mode]
        set propagation-delay {integer}
        set rp-candidate [enable|disable]
        set rp-candidate-group {string}
        set rp-candidate-interval {integer}
        set rp-candidate-priority {integer}
        set rpf-nbr-fail-back [enable|disable]
        set rpf-nbr-fail-back-filter {string}
        set state-refresh-interval {integer}
        set static-group {string}
        set ttl-threshold {integer}
    next
end
set multicast-routing [enable|disable]
config pim-sm-global
    Description: PIM sparse-mode global settings.
    set accept-register-list {string}
    set accept-source-list {string}
    set bsr-allow-quick-refresh [enable|disable]
    set bsr-candidate [enable|disable]
    set bsr-hash {integer}
    set bsr-interface {string}
    set bsr-priority {integer}
    set cisco-crp-prefix [enable|disable]
    set cisco-ignore-rp-set-priority [enable|disable]
    set cisco-register-checksum [enable|disable]
    set cisco-register-checksum-group {string}
    set join-prune-holdtime {integer}
    set message-interval {integer}
    set null-register-retries {integer}
    set pim-use-sdwan [enable|disable]
    set register-rate-limit {integer}
    set register-rp-reachability [enable|disable]
    set register-source [disable|interface|...]
    set register-source-interface {string}
    set register-source-ip {ipv4-address}
    set register-supression {integer}
    config rp-address
        Description: Statically configure RP addresses.

```



```

        edit <id>
            set group {string}
            set ip-address {ipv4-address}
        next
    end
    set rp-register-keepalive {integer}
    set spt-threshold [enable|disable]
    set spt-threshold-group {string}
    set ssm [enable|disable]
    set ssm-range {string}
end
config pim-sm-global-vrf
    Description: per-VRF PIM sparse-mode global settings.
    edit <vrf>
        set bsr-allow-quick-refresh [enable|disable]
        set bsr-candidate [enable|disable]
        set bsr-hash {integer}
        set bsr-interface {string}
        set bsr-priority {integer}
        set cisco-crp-prefix [enable|disable]
        config rp-address
            Description: Statically configure RP addresses.
            edit <id>
                set group {string}
                set ip-address {ipv4-address}
            next
        end
    next
end
set route-limit {integer}
set route-threshold {integer}
end

```

config router multicast

Parameter	Description	Type	Size	Default						
multicast-routing	Enable/disable IP multicast routing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP multicast routing.</td></tr><tr><td><i>disable</i></td><td>Disable IP multicast routing.</td></tr></table>				Option	Description	<i>enable</i>	Enable IP multicast routing.	<i>disable</i>	Disable IP multicast routing.
Option	Description									
<i>enable</i>	Enable IP multicast routing.									
<i>disable</i>	Disable IP multicast routing.									

Parameter	Description	Type	Size	Default
route-limit	Maximum number of multicast routes.	integer	Minimum value: 1 Maximum value: 2147483647	2147483647
route-threshold	Generate warnings when the number of multicast routes exceeds this number, must not be greater than route-limit.	integer	Minimum value: 1 Maximum value: 2147483647	

config interface

Parameter	Description	Type	Size	Default						
bfd	Enable/disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>disable</i></td><td>Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).</td></tr></table>	Option	Description	<i>enable</i>	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).			
Option	Description									
<i>enable</i>	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).									
<i>disable</i>	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).									
cisco-exclude-genid	Exclude GenID from hello packets (compatibility with old Cisco IOS).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Do not send GenID.</td></tr><tr><td><i>disable</i></td><td>Send GenID according to standard.</td></tr></table>	Option	Description	<i>enable</i>	Do not send GenID.	<i>disable</i>	Send GenID according to standard.			
Option	Description									
<i>enable</i>	Do not send GenID.									
<i>disable</i>	Send GenID according to standard.									
dr-priority	DR election priority.	integer	Minimum value: 1 1 Maximum value: 4294967295							
hello-holdtime	Time before old neighbor information expires (0 - 65535 sec, default = 105).	integer	Minimum value: 1 1 Maximum value: 65535	105						
hello-interval	Interval between sending PIM hello messages (0 - 65535 sec, default = 30).	integer	Minimum value: 1 1 Maximum value: 65535	30						

Parameter	Description	Type	Size	Default
multicast-flow	Acceptable source for multicast group.	string	Maximum length: 35	
name	Interface name.	string	Maximum length: 15	
neighbour-filter	Routers acknowledged as neighbor routers.	string	Maximum length: 35	
passive	Enable/disable listening to IGMP but not participating in PIM.	option	-	disable
	Option Description			
	enable	Listen only.		
	disable	Participate in PIM.		
pim-mode	PIM operation mode.	option	-	sparse-mode
	Option Description			
	sparse-mode	sparse-mode		
	dense-mode	dense-mode		
propagation-delay	Delay flooding packets on this interface (100 - 5000 msec, default = 500).	integer	Minimum value: 100 Maximum value: 5000	500
rp-candidate	Enable/disable compete to become RP in elections.	option	-	disable
	Option Description			
	enable	Compete for RP elections.		
	disable	Do not compete for RP elections.		
rp-candidate-group	Multicast groups managed by this RP.	string	Maximum length: 35	
rp-candidate-interval	RP candidate advertisement interval (1 - 16383 sec, default = 60).	integer	Minimum value: 1 Maximum value: 16383	60
rp-candidate-priority	Router's priority as RP.	integer	Minimum value: 0 Maximum value: 255	192
rpf-nbr-fail-back	Enable/disable fail back for RPF neighbor query.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable fail back for RPF neighbor query.		
	<i>disable</i>	Disable fail back for RPF neighbor query.		
rpf-nbr-fail-back-filter	Filter for fail back RPF neighbors.	string	Maximum length: 35	
state-refresh-interval	Interval between sending state-refresh packets (1 - 100 sec, default = 60).	integer	Minimum value: 1 Maximum value: 100	60
static-group	Statically set multicast groups to forward out.	string	Maximum length: 35	
ttl-threshold	Minimum TTL of multicast packets that will be forwarded (applied only to new multicast routes) (1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255	1

config igmp

Parameter	Description	Type	Size	Default
access-group	Groups IGMP hosts are allowed to join.	string	Maximum length: 35	
immediate-leave-group	Groups to drop membership for immediately after receiving IGMPv2 leave.	string	Maximum length: 35	
last-member-query-count	Number of group specific queries before removing group (2 - 7, default = 2).	integer	Minimum value: 2 Maximum value: 7	2
last-member-query-interval	Timeout between IGMPv2 leave and removing group (1 - 65535 msec, default = 1000).	integer	Minimum value: 1 Maximum value: 65535	1000
query-interval	Interval between queries to IGMP hosts (1 - 65535 sec, default = 125).	integer	Minimum value: 1 Maximum value: 65535	125
query-max-response-time	Maximum time to wait for a IGMP query response (1 - 25 sec, default = 10).	integer	Minimum value: 1 Maximum value: 25	10

Parameter	Description	Type	Size	Default								
query-timeout	Timeout between queries before becoming querying unit for network (60 - 900, default = 255).	integer	Minimum value: 60 Maximum value: 900	255								
router-alert-check	Enable/disable require IGMP packets contain router alert option.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Require Router Alert option in IGMP packets.</td></tr><tr><td>disable</td><td>don't require Router Alert option in IGMP packets</td></tr></table>				Option	Description	enable	Require Router Alert option in IGMP packets.	disable	don't require Router Alert option in IGMP packets		
Option	Description											
enable	Require Router Alert option in IGMP packets.											
disable	don't require Router Alert option in IGMP packets											
version	Maximum version of IGMP to support.	option	-	3								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>3</td><td>Version 3 and lower.</td></tr><tr><td>2</td><td>Version 2 and lower.</td></tr><tr><td>1</td><td>Version 1.</td></tr></table>				Option	Description	3	Version 3 and lower.	2	Version 2 and lower.	1	Version 1.
Option	Description											
3	Version 3 and lower.											
2	Version 2 and lower.											
1	Version 1.											

config join-group

Parameter	Description	Type	Size	Default
address	Multicast group IP address.	ipv4-address-any	Not Specified	0.0.0.0

config pim-sm-global

Parameter	Description	Type	Size	Default						
accept-register-list	Sources allowed to register packets with this Rendezvous Point (RP).	string	Maximum length: 35							
accept-source-list	Sources allowed to send multicast traffic.	string	Maximum length: 35							
bsr-allow-quick-refresh	Enable/disable accept BSR quick refresh packets from neighbors.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow quick refresh packets.</td></tr><tr><td><i>disable</i></td><td>Do not allow quick refresh packets.</td></tr></table>	Option	Description	<i>enable</i>	Allow quick refresh packets.	<i>disable</i>	Do not allow quick refresh packets.			
Option	Description									
<i>enable</i>	Allow quick refresh packets.									
<i>disable</i>	Do not allow quick refresh packets.									

Parameter	Description	Type	Size	Default						
bsr-candidate	Enable/disable allowing this router to become a bootstrap router (BSR).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow this router to function as a BSR.</td></tr><tr><td><i>disable</i></td><td>Do not allow this router to function as a BSR.</td></tr></table>	Option	Description	<i>enable</i>	Allow this router to function as a BSR.	<i>disable</i>	Do not allow this router to function as a BSR.			
Option	Description									
<i>enable</i>	Allow this router to function as a BSR.									
<i>disable</i>	Do not allow this router to function as a BSR.									
bsr-hash	BSR hash length (0 - 32, default = 10).	integer	Minimum value: 0 Maximum value: 32	10						
bsr-interface	Interface to advertise as candidate BSR.	string	Maximum length: 15							
bsr-priority	BSR priority (0 - 255, default = 0).	integer	Minimum value: 0 Maximum value: 255	0						
cisco-crp-prefix	Enable/disable making candidate RP compatible with old Cisco IOS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Do not allow sending group prefix of zero.</td></tr><tr><td><i>disable</i></td><td>Allow sending group prefix of zero.</td></tr></table>	Option	Description	<i>enable</i>	Do not allow sending group prefix of zero.	<i>disable</i>	Allow sending group prefix of zero.			
Option	Description									
<i>enable</i>	Do not allow sending group prefix of zero.									
<i>disable</i>	Allow sending group prefix of zero.									
cisco-ignore-rp-set-priority	Use only hash for RP selection (compatibility with old Cisco IOS).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Ignore RP-SET priority value.</td></tr><tr><td><i>disable</i></td><td>Do not ignore RP-SET priority value.</td></tr></table>	Option	Description	<i>enable</i>	Ignore RP-SET priority value.	<i>disable</i>	Do not ignore RP-SET priority value.			
Option	Description									
<i>enable</i>	Ignore RP-SET priority value.									
<i>disable</i>	Do not ignore RP-SET priority value.									
cisco-register-checksum	Checksum entire register packet(for old Cisco IOS compatibility).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>register checksum entire packet.</td></tr><tr><td><i>disable</i></td><td>Do not register checksum entire packet.</td></tr></table>	Option	Description	<i>enable</i>	register checksum entire packet.	<i>disable</i>	Do not register checksum entire packet.			
Option	Description									
<i>enable</i>	register checksum entire packet.									
<i>disable</i>	Do not register checksum entire packet.									

Parameter	Description	Type	Size	Default						
cisco-register-checksum-group	Cisco register checksum only these groups.	string	Maximum length: 35							
join-prune-holdtime	Join/prune holdtime (1 - 65535, default = 210).	integer	Minimum value: 1 Maximum value: 65535	210						
message-interval	Period of time between sending periodic PIM join/prune messages in seconds (1 - 65535, default = 60).	integer	Minimum value: 1 Maximum value: 65535	60						
null-register-retries	Maximum retries of null register (1 - 20, default = 1).	integer	Minimum value: 1 Maximum value: 20	1						
pim-use-sdwan	Enable/disable use of SDWAN when checking RPF neighbor and sending of REG packet.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of SDWAN when checking RPF neighbor and sending of REG packet.</td></tr><tr><td>disable</td><td>Disable use of SDWAN when checking RPF neighbor and sending of REG packet.</td></tr></table>				Option	Description	enable	Enable use of SDWAN when checking RPF neighbor and sending of REG packet.	disable	Disable use of SDWAN when checking RPF neighbor and sending of REG packet.
Option	Description									
enable	Enable use of SDWAN when checking RPF neighbor and sending of REG packet.									
disable	Disable use of SDWAN when checking RPF neighbor and sending of REG packet.									
register-rate-limit	Limit of packets/sec per source registered through this RP (0 - 65535, default = 0 which means unlimited).	integer	Minimum value: 0 Maximum value: 65535	0						
register-rp-reachability	Enable/disable check RP is reachable before registering packets.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Check target RP is unicast reachable before registering.</td></tr><tr><td>disable</td><td>Do not check RP unicast reachability.</td></tr></table>				Option	Description	enable	Check target RP is unicast reachable before registering.	disable	Do not check RP unicast reachability.
Option	Description									
enable	Check target RP is unicast reachable before registering.									
disable	Do not check RP unicast reachability.									
register-source	Override source address in register packets.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Use source address of RPF interface.		
	<i>interface</i>	Use primary IP of an interface.		
	<i>ip-address</i>	Use a local IP address.		
register-source-interface	Override with primary interface address.	string	Maximum length: 15	
register-source-ip	Override with local IP address.	ipv4-address	Not Specified	0.0.0.0
register-supression	Period of time to honor register-stop message (1 - 65535 sec, default = 60).	integer	Minimum value: 1 Maximum value: 65535	60
rp-register-keepalive	Timeout for RP receiving data on (S,G) tree (1 - 65535 sec, default = 185).	integer	Minimum value: 1 Maximum value: 65535	185
spt-threshold	Enable/disable switching to source specific trees.	option	-	enable
	Option	Description		
	<i>enable</i>	Switch to Source tree when available.		
	<i>disable</i>	Do not switch to Source tree when available.		
spt-threshold-group	Groups allowed to switch to source tree.	string	Maximum length: 35	
ssm	Enable/disable source specific multicast.	option	-	disable
	Option	Description		
	<i>enable</i>	Allow source specific multicast.		
	<i>disable</i>	Do not allow source specific multicast.		
ssm-range	Groups allowed to source specific multicast.	string	Maximum length: 35	

config rp-address

Parameter	Description	Type	Size	Default
group	Groups to use this RP.	string	Maximum length: 35	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip-address	RP router address.	ipv4-address	Not Specified	0.0.0.0

config pim-sm-global-vrf

Parameter	Description	Type	Size	Default
bsr-allow-quick-refresh	Enable/disable accept BSR quick refresh packets from neighbors.	option	-	disable
	Option			
	<i>enable</i>			Allow quick refresh packets.
	<i>disable</i>			Do not allow quick refresh packets.
bsr-candidate	Enable/disable allowing this router to become a bootstrap router (BSR).	option	-	disable
	Option			
	<i>enable</i>			Allow this router to function as a BSR.
	<i>disable</i>			Do not allow this router to function as a BSR.
bsr-hash	BSR hash length (0 - 32, default = 10).	integer	Minimum value: 0 Maximum value: 32	10
bsr-interface	Interface to advertise as candidate BSR.	string	Maximum length: 15	
bsr-priority	BSR priority (0 - 255, default = 0).	integer	Minimum value: 0 Maximum value: 255	0
cisco-crp-prefix	Enable/disable making candidate RP compatible with old Cisco IOS.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Do not allow sending group prefix of zero.		
	<i>disable</i>	Allow sending group prefix of zero.		
vrf	VRF ID.	integer	Minimum value: 1 Maximum value: 511	1886221359 **

** Values may differ between models.

config rp-address

Parameter	Description	Type	Size	Default
group	Groups to use this RP.	string	Maximum length: 35	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip-address	RP router address.	ipv4-address	Not Specified	0.0.0.0

config router multicast6

Configure IPv6 multicast.

```

config router multicast6
  Description: Configure IPv6 multicast.
  config interface
    Description: Protocol Independent Multicast (PIM) interfaces.
    edit <name>
      set hello-holdtime {integer}
      set hello-interval {integer}
    next
  end
  set multicast-pmtu [enable|disable]
  set multicast-routing [enable|disable]
  config pim-sm-global
    Description: PIM sparse-mode global settings.
    set pim-use-sdwan [enable|disable]
    set register-rate-limit {integer}
  config rp-address

```

```

        Description: Statically configured RP addresses.
        edit <id>
            set ip6-address {ipv6-address}
        next
    end
end
end

```

config router multicast6

Parameter	Description	Type	Size	Default
multicast-pmtu	Enable/disable PMTU for IPv6 multicast.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PMTU for IPv6 multicast.		
	<i>disable</i>	Disable PMTU for IPv6 multicast.		
multicast-routing	Enable/disable IPv6 multicast routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPv6 multicast routing.		
	<i>disable</i>	Disable IPv6 multicast routing.		

config interface

Parameter	Description	Type	Size	Default
hello-holdtime	Time before old neighbor information expires in seconds (1 - 65535, default = 105).	integer	Minimum value: 1 Maximum value: 65535	
hello-interval	Interval between sending PIM hello messages in seconds (1 - 65535, default = 30).	integer	Minimum value: 1 Maximum value: 65535	30
name	Interface name.	string	Maximum length: 15	

config pim-sm-global

Parameter	Description	Type	Size	Default
pim-use-sdwan	Enable/disable use of SDWAN when checking RPF neighbor and sending of REG packet.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of SDWAN when checking RPF neighbor and sending of REG packet.		
	<i>disable</i>	Disable use of SDWAN when checking RPF neighbor and sending of REG packet.		
register-rate-limit	Limit of packets/sec per source registered through this RP (0 means unlimited).	integer	Minimum value: 0 Maximum value: 65535	0

config rp-address

Parameter	Description	Type	Size	Default
id	ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip6-address	RP router IPv6 address.	ipv6-address	Not Specified	::

config router multicast-flow

Configure multicast-flow.

```
config router multicast-flow
  Description: Configure multicast-flow.
  edit <name>
    set comments {string}
    config flows
      Description: Multicast-flow entries.
      edit <id>
        set group-addr {ipv4-address-any}
        set source-addr {ipv4-address-any}
      next
    end
  next
end
```

config router multicast-flow

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

config flows

Parameter	Description	Type	Size	Default
group-addr	Multicast group IP address.	ipv4-address-any	Not Specified	0.0.0.0
id	Flow ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-addr	Multicast source IP address.	ipv4-address-any	Not Specified	0.0.0.0

config router ospf

Configure OSPF.

```
config router ospf
  Description: Configure OSPF.
  set abr-type [cisco|ibm|...]
  config area
    Description: OSPF area configuration.
    edit <id>
      set authentication [none|text|...]
      set comments {var-string}
      set default-cost {integer}
      config filter-list
        Description: OSPF area filter-list configuration.
        edit <id>
          set direction [in|out]
          set list {string}
        next
      end
    set nssa-default-information-originate [enable|always|...]
    set nssa-default-information-originate-metric {integer}
    set nssa-default-information-originate-metric-type [1|2]
```

```

set nssa-redistribution [enable|disable]
set nssa-translator-role [candidate|never|...]
config range
    Description: OSPF area range configuration.
    edit <id>
        set advertise [disable|enable]
        set prefix {ipv4-classnet-any}
        set substitute {ipv4-classnet-any}
        set substitute-status [enable|disable]
    next
end
set shortcut [disable|enable|...]
set stub-type [no-summary|summary]
set type [regular|nssa|...]
config virtual-link
    Description: OSPF virtual link configuration.
    edit <name>
        set authentication [none|text|...]
        set authentication-key {password}
        set dead-interval {integer}
        set hello-interval {integer}
        set keychain {string}
        config md5-keys
            Description: MD5 key.
            edit <id>
                set key-string {password}
            next
        end
        set peer {ipv4-address-any}
        set retransmit-interval {integer}
        set transmit-delay {integer}
    next
end
next
end
set auto-cost-ref-bandwidth {integer}
set bfd [enable|disable]
set database-overflow [enable|disable]
set database-overflow-max-lsas {integer}
set database-overflow-time-to-recover {integer}
set default-information-metric {integer}
set default-information-metric-type [1|2]
set default-information-originate [enable|always|...]
set default-information-route-map {string}
set default-metric {integer}
set distance {integer}
set distance-external {integer}
set distance-inter-area {integer}
set distance-intra-area {integer}
config distribute-list
    Description: Distribute list configuration.
    edit <id>

```

```

        set access-list {string}
        set protocol [connected|static|...]
    next
end
set distribute-list-in {string}
set distribute-route-map-in {string}
set log-neighbour-changes [enable|disable]
set lsa-refresh-interval {integer}
config neighbor
    Description: OSPF neighbor configuration are used when OSPF runs on non-broadcast media.
    edit <id>
        set cost {integer}
        set ip {ipv4-address}
        set poll-interval {integer}
        set priority {integer}
    next
end
config network
    Description: OSPF network configuration.
    edit <id>
        set area {ipv4-address-any}
        set comments {var-string}
        set prefix {ipv4-classnet}
    next
end
config ospf-interface
    Description: OSPF interface configuration.
    edit <name>
        set authentication [none|text|...]
        set authentication-key {password}
        set bfd [global|enable|...]
        set comments {var-string}
        set cost {integer}
        set database-filter-out [enable|disable]
        set dead-interval {integer}
        set hello-interval {integer}
        set hello-multiplier {integer}
        set interface {string}
        set ip {ipv4-address}
        set keychain {string}
        set linkdown-fast-failover [enable|disable]
        config md5-keys
            Description: MD5 key.
            edit <id>
                set key-string {password}
            next
        end
        set mtu {integer}
        set mtu-ignore [enable|disable]
        set network-type [broadcast|non-broadcast|...]
        set prefix-length {integer}
        set priority {integer}
    end
end

```

```

        set resync-timeout {integer}
        set retransmit-interval {integer}
        set status [disable|enable]
        set transmit-delay {integer}
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration. Read-only.
    edit <name>
        set metric {integer}
        set metric-type [1|2]
        set routemap {string}
        set status [enable|disable]
        set tag {integer}
    next
end
set restart-mode [none|lls|...]
set restart-on-topology-change [enable|disable]
set restart-period {integer}
set rfc1583-compatible [enable|disable]
set router-id {ipv4-address-any}
set spf-timers {user}
config summary-address
    Description: IP address summary configuration.
    edit <id>
        set advertise [disable|enable]
        set prefix {ipv4-classnet}
        set tag {integer}
    next
end
end
end

```

config router ospf

Parameter	Description	Type	Size	Default										
abr-type	Area border router type.	option	-	standard										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cisco</td><td>Cisco.</td></tr><tr><td>ibm</td><td>IBM.</td></tr><tr><td>shortcut</td><td>Shortcut.</td></tr><tr><td>standard</td><td>Standard.</td></tr></table>				Option	Description	cisco	Cisco.	ibm	IBM.	shortcut	Shortcut.	standard	Standard.
	Option	Description												
	cisco	Cisco.												
	ibm	IBM.												
	shortcut	Shortcut.												
standard	Standard.													

Parameter	Description	Type	Size	Default						
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000	1000						
bfd	Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
database-overflow	Enable/disable database overflow.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
database-overflow-max-lsas	Database overflow maximum LSAs.	integer	Minimum value: 0 Maximum value: 4294967295	10000						
database-overflow-time-to-recover	Database overflow time to recover (sec).	integer	Minimum value: 0 Maximum value: 65535	300						
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214	10						
default-information-metric-type	Default information metric type.	option	-	2						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1</i></td><td>Type 1.</td></tr><tr><td><i>2</i></td><td>Type 2.</td></tr></table>	Option	Description	<i>1</i>	Type 1.	<i>2</i>	Type 2.			
Option	Description									
<i>1</i>	Type 1.									
<i>2</i>	Type 2.									
default-information-originate	Enable/disable generation of default route.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable setting.		
	always	Always advertise the default router.		
	disable	Disable setting.		
default-information-route-map	Default information route map.	string	Maximum length: 35	
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214	10
distance	Distance of the route.	integer	Minimum value: 1 Maximum value: 255	110
distance-external	Administrative external distance.	integer	Minimum value: 1 Maximum value: 255	110
distance-inter-area	Administrative inter-area distance.	integer	Minimum value: 1 Maximum value: 255	110
distance-intra-area	Administrative intra-area distance.	integer	Minimum value: 1 Maximum value: 255	110
distribute-list-in	Filter incoming routes.	string	Maximum length: 35	
distribute-route-map-in	Filter incoming external routes by route-map.	string	Maximum length: 35	
log-neighbour-changes	Log of OSPF neighbor changes.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
lsa-refresh-interval	The minimal OSPF LSA update time interval	integer	Minimum value: 0 Maximum value: 5	5

Parameter	Description	Type	Size	Default								
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79									
restart-mode	OSPF restart mode (graceful or LLS).	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Hitless restart disabled.</td></tr><tr><td><i>lls</i></td><td>LLS mode.</td></tr><tr><td><i>graceful-restart</i></td><td>Graceful Restart Mode.</td></tr></table>	Option	Description	<i>none</i>	Hitless restart disabled.	<i>lls</i>	LLS mode.	<i>graceful-restart</i>	Graceful Restart Mode.			
Option	Description											
<i>none</i>	Hitless restart disabled.											
<i>lls</i>	LLS mode.											
<i>graceful-restart</i>	Graceful Restart Mode.											
restart-on-topology-change	Enable/disable continuing graceful restart upon topology change.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Continue graceful restart upon topology change.</td></tr><tr><td><i>disable</i></td><td>Exit graceful restart upon topology change.</td></tr></table>	Option	Description	<i>enable</i>	Continue graceful restart upon topology change.	<i>disable</i>	Exit graceful restart upon topology change.					
Option	Description											
<i>enable</i>	Continue graceful restart upon topology change.											
<i>disable</i>	Exit graceful restart upon topology change.											
restart-period	Graceful restart period.	integer	Minimum value: 120 Maximum value: 3600									
rfc1583-compatible	Enable/disable RFC1583 compatibility.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
router-id	Router ID.	ipv4-address-any	Not Specified	0.0.0.0								
spf-timers	SPF calculation frequency.	user	Not Specified									

config area

Parameter	Description	Type	Size	Default				
authentication	Authentication type.	option	-	none				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr></table>				Option	Description	<i>none</i>	None.
	Option	Description						
<i>none</i>	None.							

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>message-digest</i></td><td>Message digest.</td></tr></table>	Option	Description	<i>text</i>	Text.	<i>message-digest</i>	Message digest.					
	Option	Description										
	<i>text</i>	Text.										
<i>message-digest</i>	Message digest.											
comments	Comment.	var-string	Maximum length: 255									
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 4294967295	10								
id	Area entry IP address.	ipv4-address-any	Not Specified	0.0.0.0								
nssa-default-information-originate	Redistribute, advertise, or do not originate Type-7 default route into NSSA area.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Redistribute Type-7 default route from routing table.</td></tr><tr><td><i>always</i></td><td>Advertise a self-originated Type-7 default route.</td></tr><tr><td><i>disable</i></td><td>Do not advertise Type-7 default route.</td></tr></table>	Option	Description	<i>enable</i>	Redistribute Type-7 default route from routing table.	<i>always</i>	Advertise a self-originated Type-7 default route.	<i>disable</i>	Do not advertise Type-7 default route.			
	Option	Description										
	<i>enable</i>	Redistribute Type-7 default route from routing table.										
	<i>always</i>	Advertise a self-originated Type-7 default route.										
<i>disable</i>	Do not advertise Type-7 default route.											
nssa-default-information-originate-metric	OSPF default metric.	integer	Minimum value: 0 Maximum value: 16777214	10								
nssa-default-information-originate-metric-type	OSPF metric type for default routes.	option	-	2								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1</i></td><td>Type 1.</td></tr><tr><td><i>2</i></td><td>Type 2.</td></tr></table>	Option	Description	<i>1</i>	Type 1.	<i>2</i>	Type 2.					
	Option	Description										
	<i>1</i>	Type 1.										
<i>2</i>	Type 2.											
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable redistribute into NSSA area.		
	<i>disable</i>	Disable redistribute into NSSA area.		
nssa-translator-role	NSSA translator role type.	option	-	candidate
	Option	Description		
	<i>candidate</i>	Candidate.		
	<i>never</i>	Never.		
	<i>always</i>	Always.		
shortcut	Enable/disable shortcut option.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable shortcut option.		
	<i>enable</i>	Enable shortcut option.		
	<i>default</i>	Default shortcut option.		
stub-type	Stub summary setting.	option	-	summary
	Option	Description		
	<i>no-summary</i>	No summary.		
	<i>summary</i>	Summary.		
type	Area type setting.	option	-	regular
	Option	Description		
	<i>regular</i>	Regular.		
	<i>nssa</i>	NSSA.		
	<i>stub</i>	Stub.		

config filter-list

Parameter	Description	Type	Size	Default
direction	Direction.	option	-	out

Parameter	Description	Type	Size	Default
	Option Description			
	<i>in</i>	In.		
	<i>out</i>	Out.		
id	Filter list entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
list	Access-list or prefix-list name.	string	Maximum length: 35	

config range

Parameter	Description	Type	Size	Default
advertise	Enable/disable advertise status.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable advertise status.		
	<i>enable</i>	Enable advertise status.		
id	Range entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
prefix	Prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
substitute	Substitute prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
substitute-status	Enable/disable substitute status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable substitute status.		
	<i>disable</i>	Disable substitute status.		

config virtual-link

Parameter	Description	Type	Size	Default								
authentication	Authentication type.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>message-digest</i></td><td>Message digest.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>message-digest</i>	Message digest.			
	Option	Description										
	<i>none</i>	None.										
	<i>text</i>	Text.										
<i>message-digest</i>	Message digest.											
authentication-key	Authentication key.	password	Not Specified									
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	40								
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	10								
keychain	Message-digest key-chain name.	string	Maximum length: 35									
name	Virtual link entry name.	string	Maximum length: 35									
peer	Peer IP.	ipv4-address-any	Not Specified	0.0.0.0								
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5								
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1								

config md5-keys

Parameter	Description	Type	Size	Default
id	Key ID (1 - 255).	integer	Minimum value: 1 Maximum value: 255	0
key-string	Password for the key.	password	Not Specified	

config distribute-list

Parameter	Description	Type	Size	Default
access-list	Access list name.	string	Maximum length: 35	
id	Distribute list entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Protocol type.	option	-	connected
	Option	Description		
	connected	Connected type.		
	static	Static type.		
	rip	RIP type.		

config neighbor

Parameter	Description	Type	Size	Default
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
id	Neighbor entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Interface IP address of the neighbor.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535	10
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1

config network

Parameter	Description	Type	Size	Default
area	Attach the network to area.	ipv4-address-any	Not Specified	0.0.0.0
comments	Comment.	var-string	Maximum length: 255	
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config ospf-interface

Parameter	Description	Type	Size	Default								
authentication	Authentication type.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>message-digest</i></td><td>Message digest.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>message-digest</i>	Message digest.			
Option	Description											
<i>none</i>	None.											
<i>text</i>	Text.											
<i>message-digest</i>	Message digest.											
authentication-key	Authentication key.	password	Not Specified									
bfd	Bidirectional Forwarding Detection (BFD).	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Follow global configuration.</td></tr></table>	Option	Description	<i>global</i>	Follow global configuration.							
Option	Description											
<i>global</i>	Follow global configuration.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable BFD on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable BFD on this interface.</td></tr></table>				Option	Description	<i>enable</i>	Enable BFD on this interface.	<i>disable</i>	Disable BFD on this interface.
	Option	Description								
	<i>enable</i>	Enable BFD on this interface.								
<i>disable</i>	Disable BFD on this interface.									
comments	Comment.	var-string	Maximum length: 255							
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0						
database-filter-out	Enable/disable control of flooding out LSAs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
dead-interval	Dead interval.	integer	Minimum value: 0 Maximum value: 65535	0						
hello-interval	Hello interval.	integer	Minimum value: 0 Maximum value: 65535	0						
hello-multiplier	Number of hello packets within dead interval.	integer	Minimum value: 3 Maximum value: 10	0						
interface	Configuration interface name.	string	Maximum length: 15							
ip	IP address.	ipv4-address	Not Specified	0.0.0.0						
keychain	Message-digest key-chain name.	string	Maximum length: 35							
linkdown-fast-failover	Enable/disable fast link failover.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable fast failover for VLAN interfaces.		
	<i>disable</i>	Disable fast failover for VLAN interfaces.		
mtu	MTU for database description packets.	integer	Minimum value: 576 Maximum value: 65535	0
mtu-ignore	Enable/disable ignore MTU.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
name	Interface entry name.	string	Maximum length: 35	
network-type	Network type.	option	-	broadcast
	Option	Description		
	<i>broadcast</i>	Broadcast.		
	<i>non-broadcast</i>	Non-broadcast.		
	<i>point-to-point</i>	Point-to-point.		
	<i>point-to-multipoint</i>	Point-to-multipoint.		
	<i>point-to-multipoint-non-broadcast</i>	Point-to-multipoint and non-broadcast.		
prefix-length	Prefix length.	integer	Minimum value: 0 Maximum value: 32	0
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1

Parameter	Description	Type	Size	Default
resync-timeout	Graceful restart neighbor resynchronization timeout.	integer	Minimum value: 1 Maximum value: 3600	40
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
status	Enable/disable status.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1

config md5-keys

Parameter	Description	Type	Size	Default
id	Key ID (1 - 255).	integer	Minimum value: 1 Maximum value: 255	0
key-string	Password for the key.	password	Not Specified	

config redistribute

Parameter	Description	Type	Size	Default
metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214	0
metric-type	Metric type.	option	-	2

Parameter	Description	Type	Size	Default							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Type 1.</td></tr><tr><td>2</td><td>Type 2.</td></tr></table>		Option	Description	1	Type 1.	2	Type 2.			
	Option	Description									
	1	Type 1.									
2	Type 2.										
name	Redistribute name.	string	Maximum length: 35								
routemap	Route map name.	string	Maximum length: 35								
status	Status.	option	-	disable							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>		Option	Description	enable	Enable setting.	disable	Disable setting.			
	Option	Description									
	enable	Enable setting.									
disable	Disable setting.										
tag	Tag value.	integer	Minimum value: 0 0 Maximum value: 4294967295								

config summary-address

Parameter	Description	Type	Size	Default						
advertise	Enable/disable advertise status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable advertise status.</td></tr><tr><td><i>enable</i></td><td>Enable advertise status.</td></tr></table>				Option	Description	<i>disable</i>	Disable advertise status.	<i>enable</i>	Enable advertise status.
	Option	Description								
	<i>disable</i>	Disable advertise status.								
<i>enable</i>	Enable advertise status.									
id	Summary address entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
prefix	Prefix.	ipv4- classnet	Not Specified	0.0.0.0 0.0.0.0						
tag	Tag value.	integer	Minimum value: 0 0 Maximum value: 4294967295							

config router ospf6

Configure IPv6 OSPF.

```
config router ospf6
  Description: Configure IPv6 OSPF.
  set abr-type [cisco|ibm|...]
  config area
    Description: OSPF6 area configuration.
    edit <id>
      set authentication [none|ah|...]
      set default-cost {integer}
      set ipsec-auth-alg [md5|sha1|...]
      set ipsec-enc-alg [null|des|...]
      config ipsec-keys
        Description: IPsec authentication and encryption keys.
        edit <spi>
          set auth-key {password}
          set enc-key {password}
        next
      end
      set key-rollover-interval {integer}
      set nssa-default-information-originate [enable|disable]
      set nssa-default-information-originate-metric {integer}
      set nssa-default-information-originate-metric-type [1|2]
      set nssa-redistribution [enable|disable]
      set nssa-translator-role [candidate|never|...]
      config range
        Description: OSPF6 area range configuration.
        edit <id>
          set advertise [disable|enable]
          set prefix6 {ipv6-network}
        next
      end
      set stub-type [no-summary|summary]
      set type [regular|nssa|...]
      config virtual-link
        Description: OSPF6 virtual link configuration.
        edit <name>
          set authentication [none|ah|...]
          set dead-interval {integer}
          set hello-interval {integer}
          set ipsec-auth-alg [md5|sha1|...]
          set ipsec-enc-alg [null|des|...]
          config ipsec-keys
            Description: IPsec authentication and encryption keys.
            edit <spi>
              set auth-key {password}
              set enc-key {password}
            next
          end
        end
      end
    end
  end
```

```

        set key-rollover-interval {integer}
        set peer {ipv4-address-any}
        set retransmit-interval {integer}
        set transmit-delay {integer}
    next
end
next
end
set auto-cost-ref-bandwidth {integer}
set bfd [enable|disable]
set default-information-metric {integer}
set default-information-metric-type [1|2]
set default-information-originate [enable|always|...]
set default-information-route-map {string}
set default-metric {integer}
set log-neighbour-changes [enable|disable]
config ospf6-interface
    Description: OSPF6 interface configuration.
    edit <name>
        set area-id {ipv4-address-any}
        set authentication [none|ah|...]
        set bfd [global|enable|...]
        set cost {integer}
        set dead-interval {integer}
        set hello-interval {integer}
        set interface {string}
        set ipsec-auth-alg [md5|sha1|...]
        set ipsec-enc-alg [null|des|...]
        config ipsec-keys
            Description: IPsec authentication and encryption keys.
            edit <spi>
                set auth-key {password}
                set enc-key {password}
            next
        end
        set key-rollover-interval {integer}
        set mtu {integer}
        set mtu-ignore [enable|disable]
        config neighbor
            Description: OSPFv3 neighbors are used when OSPFv3 runs on non-broadcast media.
            edit <ip6>
                set cost {integer}
                set poll-interval {integer}
                set priority {integer}
            next
        end
        set network-type [broadcast|point-to-point|...]
        set priority {integer}
        set retransmit-interval {integer}
        set status [disable|enable]
        set transmit-delay {integer}
    next

```

```

end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration. Read-only.
    edit <name>
        set metric {integer}
        set metric-type [1|2]
        set routemap {string}
        set status [enable|disable]
    next
end
set restart-mode [none|graceful-restart]
set restart-on-topology-change [enable|disable]
set restart-period {integer}
set router-id {ipv4-address-any}
set spf-timers {user}
config summary-address
    Description: IPv6 address summary configuration.
    edit <id>
        set advertise [disable|enable]
        set prefix6 {ipv6-network}
        set tag {integer}
    next
end
end
end

```

config router ospf6

Parameter	Description	Type	Size	Default								
abr-type	Area border router type.	option	-	standard								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cisco</td><td>Cisco.</td></tr><tr><td>ibm</td><td>IBM.</td></tr><tr><td>standard</td><td>Standard.</td></tr></table>				Option	Description	cisco	Cisco.	ibm	IBM.	standard	Standard.
	Option	Description										
	cisco	Cisco.										
	ibm	IBM.										
standard	Standard.											
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000	1000								
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>disable</i></td><td>Disable Bidirectional Forwarding Detection (BFD).</td></tr></table>	Option	Description	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).					
	Option	Description										
	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).										
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).											
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214	10								
default-information-metric-type	Default information metric type.	option	-	2								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1</i></td><td>Type 1.</td></tr><tr><td><i>2</i></td><td>Type 2.</td></tr></table>	Option	Description	<i>1</i>	Type 1.	<i>2</i>	Type 2.					
	Option	Description										
	<i>1</i>	Type 1.										
<i>2</i>	Type 2.											
default-information-originate	Enable/disable generation of default route.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>always</i></td><td>Always advertise the default router.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>always</i>	Always advertise the default router.	<i>disable</i>	Disable setting.			
	Option	Description										
	<i>enable</i>	Enable setting.										
	<i>always</i>	Always advertise the default router.										
<i>disable</i>	Disable setting.											
default-information-route-map	Default information route map.	string	Maximum length: 35									
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214	10								
log-neighbour-changes	Log OSPFv3 neighbor changes.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.							
	Option	Description										
<i>enable</i>	Enable setting.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.					
	Option	Description								
<i>disable</i>	Disable setting.									
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79							
restart-mode	OSPFv3 restart mode (graceful or none).	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Disable hitless restart.</td></tr><tr><td><i>graceful-restart</i></td><td>Enable graceful restart mode.</td></tr></table>	Option	Description	<i>none</i>	Disable hitless restart.	<i>graceful-restart</i>	Enable graceful restart mode.			
	Option	Description								
	<i>none</i>	Disable hitless restart.								
<i>graceful-restart</i>	Enable graceful restart mode.									
restart-on-topology-change	Enable/disable continuing graceful restart upon topology change.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Continue graceful restart upon topology change.</td></tr><tr><td><i>disable</i></td><td>Exit graceful restart upon topology change.</td></tr></table>	Option	Description	<i>enable</i>	Continue graceful restart upon topology change.	<i>disable</i>	Exit graceful restart upon topology change.			
	Option	Description								
	<i>enable</i>	Continue graceful restart upon topology change.								
<i>disable</i>	Exit graceful restart upon topology change.									
restart-period	Graceful restart period in seconds.	integer	Minimum value: 1 Maximum value: 3600	120						
router-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified	0.0.0.0						
spf-timers	SPF calculation frequency.	user	Not Specified							

config area

Parameter	Description	Type	Size	Default
authentication	Authentication mode.	option	-	none
	Option	Description		
	<i>none</i>	Disable authentication.		
	<i>ah</i>	Authentication Header.		
	<i>esp</i>	Encapsulating Security Payload.		

Parameter	Description	Type	Size	Default														
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 16777215	10														
id	Area entry IP address.	ipv4-address-any	Not Specified	0.0.0.0														
ipsec-auth-alg	Authentication algorithm.	option	-	md5														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>md5</td><td>MD5.</td></tr><tr><td>sha1</td><td>SHA1.</td></tr><tr><td>sha256</td><td>SHA256.</td></tr><tr><td>sha384</td><td>SHA384.</td></tr><tr><td>sha512</td><td>SHA512.</td></tr></table>	Option	Description	md5	MD5.	sha1	SHA1.	sha256	SHA256.	sha384	SHA384.	sha512	SHA512.					
Option	Description																	
md5	MD5.																	
sha1	SHA1.																	
sha256	SHA256.																	
sha384	SHA384.																	
sha512	SHA512.																	
ipsec-enc-alg	Encryption algorithm.	option	-	null														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>null</td><td>No encryption.</td></tr><tr><td>des</td><td>DES.</td></tr><tr><td>3des</td><td>3DES.</td></tr><tr><td>aes128</td><td>AES128.</td></tr><tr><td>aes192</td><td>AES192.</td></tr><tr><td>aes256</td><td>AES256.</td></tr></table>	Option	Description	null	No encryption.	des	DES.	3des	3DES.	aes128	AES128.	aes192	AES192.	aes256	AES256.			
Option	Description																	
null	No encryption.																	
des	DES.																	
3des	3DES.																	
aes128	AES128.																	
aes192	AES192.																	
aes256	AES256.																	
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300														
nssa-default-information-originate	Enable/disable originate type 7 default into NSSA area.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable originate type 7 default into NSSA area.</td></tr><tr><td>disable</td><td>Disable originate type 7 default into NSSA area.</td></tr></table>	Option	Description	enable	Enable originate type 7 default into NSSA area.	disable	Disable originate type 7 default into NSSA area.											
Option	Description																	
enable	Enable originate type 7 default into NSSA area.																	
disable	Disable originate type 7 default into NSSA area.																	

Parameter	Description	Type	Size	Default								
nssa-default-information-originate-metric	OSPFv3 default metric.	integer	Minimum value: 0 Maximum value: 16777214	10								
nssa-default-information-originate-metric-type	OSPFv3 metric type for default routes.	option	-	2								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Type 1.</td></tr><tr><td>2</td><td>Type 2.</td></tr></table>	Option	Description	1	Type 1.	2	Type 2.					
Option	Description											
1	Type 1.											
2	Type 2.											
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable redistribute into NSSA area.</td></tr><tr><td>disable</td><td>Disable redistribute into NSSA area.</td></tr></table>	Option	Description	enable	Enable redistribute into NSSA area.	disable	Disable redistribute into NSSA area.					
Option	Description											
enable	Enable redistribute into NSSA area.											
disable	Disable redistribute into NSSA area.											
nssa-translator-role	NSSA translator role type.	option	-	candidate								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>candidate</td><td>Candidate.</td></tr><tr><td>never</td><td>Never.</td></tr><tr><td>always</td><td>Always.</td></tr></table>	Option	Description	candidate	Candidate.	never	Never.	always	Always.			
Option	Description											
candidate	Candidate.											
never	Never.											
always	Always.											
stub-type	Stub summary setting.	option	-	summary								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no-summary</td><td>No summary.</td></tr><tr><td>summary</td><td>Summary.</td></tr></table>	Option	Description	no-summary	No summary.	summary	Summary.					
Option	Description											
no-summary	No summary.											
summary	Summary.											
type	Area type setting.	option	-	regular								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>regular</td><td>Regular.</td></tr><tr><td>nssa</td><td>NSSA.</td></tr><tr><td>stub</td><td>Stub.</td></tr></table>	Option	Description	regular	Regular.	nssa	NSSA.	stub	Stub.			
Option	Description											
regular	Regular.											
nssa	NSSA.											
stub	Stub.											

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	
spi	Security Parameters Index.	integer	Minimum value: 0 256 Maximum value: 4294967295	

config range

Parameter	Description	Type	Size	Default
advertise	Enable/disable advertise status.	option	-	enable
	Option	Description		
	disable	disable		
	enable	enable		
id	Range entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0

config virtual-link

Parameter	Description	Type	Size	Default
authentication	Authentication mode.	option	-	area
	Option	Description		
	<i>none</i>	Disable authentication.		
	<i>ah</i>	Authentication Header.		
	<i>esp</i>	Encapsulating Security Payload.		
	<i>area</i>	Use the routing area's authentication configuration.		

Parameter	Description	Type	Size	Default
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	40
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	10
ipsec-auth-alg	Authentication algorithm.	option	-	md5
	Option Description			
	md5	MD5.		
	sha1	SHA1.		
	sha256	SHA256.		
	sha384	SHA384.		
	sha512	SHA512.		
	ipsec-enc-alg	Encryption algorithm.	option	-
	Option Description			
	null	No encryption.		
	des	DES.		
	3des	3DES.		
	aes128	AES128.		
	aes192	AES192.		
	aes256	AES256.		
	key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000
name	Virtual link entry name.	string	Maximum length: 35	
peer	A.B.C.D, peer router ID.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	
spi	Security Parameters Index.	integer	Minimum value: 0 256 Maximum value: 4294967295	

config ospf6-interface

Parameter	Description	Type	Size	Default										
area-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified	0.0.0.0										
authentication	Authentication mode.	option	-	area										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Disable authentication.</td></tr><tr><td><i>ah</i></td><td>Authentication Header.</td></tr><tr><td><i>esp</i></td><td>Encapsulating Security Payload.</td></tr><tr><td><i>area</i></td><td>Use the routing area's authentication configuration.</td></tr></table>				Option	Description	<i>none</i>	Disable authentication.	<i>ah</i>	Authentication Header.	<i>esp</i>	Encapsulating Security Payload.	<i>area</i>	Use the routing area's authentication configuration.
	Option	Description												
	<i>none</i>	Disable authentication.												
	<i>ah</i>	Authentication Header.												
	<i>esp</i>	Encapsulating Security Payload.												
<i>area</i>	Use the routing area's authentication configuration.													
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	global										

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Use global configuration of Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>enable</i></td><td>Enable Bidirectional Forwarding Detection (BFD) on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable Bidirectional Forwarding Detection (BFD) on this interface.</td></tr></table>	Option	Description	<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.							
	Option	Description														
	<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).														
	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.														
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.															
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0												
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	0												
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	0												
interface	Configuration interface name.	string	Maximum length: 15													
ipsec-auth-alg	Authentication algorithm.	option	-	md5												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>md5</i></td><td>MD5.</td></tr><tr><td><i>sha1</i></td><td>SHA1.</td></tr><tr><td><i>sha256</i></td><td>SHA256.</td></tr><tr><td><i>sha384</i></td><td>SHA384.</td></tr><tr><td><i>sha512</i></td><td>SHA512.</td></tr></table>	Option	Description	<i>md5</i>	MD5.	<i>sha1</i>	SHA1.	<i>sha256</i>	SHA256.	<i>sha384</i>	SHA384.	<i>sha512</i>	SHA512.			
	Option	Description														
	<i>md5</i>	MD5.														
	<i>sha1</i>	SHA1.														
	<i>sha256</i>	SHA256.														
	<i>sha384</i>	SHA384.														
<i>sha512</i>	SHA512.															
ipsec-enc-alg	Encryption algorithm.	option	-	null												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null</i></td><td>No encryption.</td></tr><tr><td><i>des</i></td><td>DES.</td></tr><tr><td><i>3des</i></td><td>3DES.</td></tr><tr><td><i>aes128</i></td><td>AES128.</td></tr></table>	Option	Description	<i>null</i>	No encryption.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.					
	Option	Description														
	<i>null</i>	No encryption.														
	<i>des</i>	DES.														
	<i>3des</i>	3DES.														
<i>aes128</i>	AES128.															

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aes192</i></td><td>AES192.</td></tr><tr><td><i>aes256</i></td><td>AES256.</td></tr></table>	Option	Description	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.									
	Option	Description														
	<i>aes192</i>	AES192.														
<i>aes256</i>	AES256.															
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300												
mtu	MTU for OSPFv3 packets.	integer	Minimum value: 576 Maximum value: 65535	0												
mtu-ignore	Enable/disable ignoring MTU field in DBD packets.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Ignore MTU field in DBD packets.</td></tr><tr><td><i>disable</i></td><td>Do not ignore MTU field in DBD packets.</td></tr></table>	Option	Description	<i>enable</i>	Ignore MTU field in DBD packets.	<i>disable</i>	Do not ignore MTU field in DBD packets.									
	Option	Description														
	<i>enable</i>	Ignore MTU field in DBD packets.														
<i>disable</i>	Do not ignore MTU field in DBD packets.															
name	Interface entry name.	string	Maximum length: 35													
network-type	Network type.	option	-	broadcast												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>broadcast</i></td><td>broadcast</td></tr><tr><td><i>point-to-point</i></td><td>point-to-point</td></tr><tr><td><i>non-broadcast</i></td><td>non-broadcast</td></tr><tr><td><i>point-to-multipoint</i></td><td>point-to-multipoint</td></tr><tr><td><i>point-to-multipoint-non-broadcast</i></td><td>point-to-multipoint and non-broadcast.</td></tr></table>	Option	Description	<i>broadcast</i>	broadcast	<i>point-to-point</i>	point-to-point	<i>non-broadcast</i>	non-broadcast	<i>point-to-multipoint</i>	point-to-multipoint	<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.			
	Option	Description														
	<i>broadcast</i>	broadcast														
	<i>point-to-point</i>	point-to-point														
	<i>non-broadcast</i>	non-broadcast														
	<i>point-to-multipoint</i>	point-to-multipoint														
<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.															
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1												

Parameter	Description	Type	Size	Default
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
status	Enable/disable OSPF6 routing on this interface.	option	-	enable
	Option	Description		
	disable	Disable OSPF6 routing.		
	enable	Enable OSPF6 routing.		
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	
spi	Security Parameters Index.	integer	Minimum value: 0 256 Maximum value: 4294967295	0

config neighbor

Parameter	Description	Type	Size	Default
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
ip6	IPv6 link local address of the neighbor.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535	10
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1

config redistribute

Parameter	Description	Type	Size	Default						
metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214	0						
metric-type	Metric type.	option	-	2						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Type 1.</td></tr><tr><td>2</td><td>Type 2.</td></tr></table>				Option	Description	1	Type 1.	2	Type 2.
	Option	Description								
	1	Type 1.								
2	Type 2.									
name	Redistribute name.	string	Maximum length: 35							
routemap	Route map name.	string	Maximum length: 35							
status	Status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									

config summary-address

Parameter	Description	Type	Size	Default
advertise	Enable/disable advertise status.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	disable	disable		
	enable	enable		
id	Summary address entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0
tag	Tag value.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config router policy

Configure IPv4 routing policies.

```

config router policy
  Description: Configure IPv4 routing policies.
  edit <seq-num>
    set action [deny|permit]
    set comments {var-string}
    set dst <subnet1>, <subnet2>, ...
    set dst-negate [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set end-port {integer}
    set end-source-port {integer}
    set gateway {ipv4-address}
    set groups <name1>, <name2>, ...
    set input-device <name1>, <name2>, ...
    set input-device-negate [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-id <id1>, <id2>, ...
    set output-device {string}
    set protocol {integer}
    set src <subnet1>, <subnet2>, ...
    set src-negate [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set start-port {integer}
    set start-source-port {integer}
    set status [enable|disable]
    set tos {user}
    set tos-mask {user}

```

```

        set users <name1>, <name2>, ...
    next
end

```

config router policy

Parameter	Description	Type	Size	Default
action	Action of the policy route.	option	-	permit
	Option	Description		
	<i>deny</i>	Do not search policy route table.		
	<i>permit</i>	Use this policy route for forwarding.		
comments	Optional comments.	var-string	Maximum length: 255	
dst <subnet>	Destination IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79	
dst-negate	Enable/disable negating destination address match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable destination address negation.		
	<i>disable</i>	Disable destination address negation.		
dstaddr <name>	Destination address name. Address/group name.	string	Maximum length: 79	
end-port	End destination port number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535	65535
end-source-port	End source port number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535	65535
gateway	IP address of the gateway.	ipv4-address	Not Specified	0.0.0.0
groups <name>	List of user groups. Group name.	string	Maximum length: 79	
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79	
input-device-negate	Enable/disable negation of input device match.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negation of input device match.</td></tr><tr><td><i>disable</i></td><td>Disable negation of input device match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negation of input device match.	<i>disable</i>	Disable negation of input device match.			
	Option	Description								
	<i>enable</i>	Enable negation of input device match.								
<i>disable</i>	Disable negation of input device match.									
internet-service-custom <name>	Custom Destination Internet Service name. Custom Destination Internet Service name.	string	Maximum length: 79							
internet-service-id <id>	Destination Internet Service ID. Destination Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295							
output-device	Outgoing interface name.	string	Maximum length: 35							
protocol	Protocol number (0 - 255).	integer	Minimum value: 0 Maximum value: 255							
seq-num	Sequence number(1-65535).	integer	Minimum value: 0 Maximum value: 65535							
src <subnet>	Source IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79							
src-negate	Enable/disable negating source address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negation.</td></tr><tr><td><i>disable</i></td><td>Disable source address negation.</td></tr></table>	Option	Description	<i>enable</i>	Enable source address negation.	<i>disable</i>	Disable source address negation.			
	Option	Description								
	<i>enable</i>	Enable source address negation.								
<i>disable</i>	Disable source address negation.									
srcaddr <name>	Source address name. Address/group name.	string	Maximum length: 79							
start-port	Start destination port number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535							
start-source-port	Start source port number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535							
status	Enable/disable this policy route.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable this policy route.		
	<i>disable</i>	Disable this policy route.		
tos	Type of service bit pattern.	user	Not Specified	
tos-mask	Type of service evaluated bits.	user	Not Specified	
users <name>	List of users. User name.	string	Maximum length: 79	

config router policy6

Configure IPv6 routing policies.

```

config router policy6
  Description: Configure IPv6 routing policies.
  edit <seq-num>
    set action [deny|permit]
    set comments {var-string}
    set dst <addr61>, <addr62>, ...
    set dst-negate [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set end-port {integer}
    set end-source-port {integer}
    set gateway {ipv6-address}
    set groups <name1>, <name2>, ...
    set input-device <name1>, <name2>, ...
    set input-device-negate [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-id <id1>, <id2>, ...
    set output-device {string}
    set protocol {integer}
    set src <addr61>, <addr62>, ...
    set src-negate [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set start-port {integer}
    set start-source-port {integer}
    set status [enable|disable]
    set tos {user}
    set tos-mask {user}
    set users <name1>, <name2>, ...
  next
end

```

config router policy6

Parameter	Description	Type	Size	Default						
action	Action of the policy route.	option	-	permit						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>deny</i></td><td>Do not search policy route table.</td></tr><tr><td><i>permit</i></td><td>Use this policy route for forwarding.</td></tr></table>	Option	Description	<i>deny</i>	Do not search policy route table.	<i>permit</i>	Use this policy route for forwarding.			
Option	Description									
<i>deny</i>	Do not search policy route table.									
<i>permit</i>	Use this policy route for forwarding.									
comments	Optional comments.	var-string	Maximum length: 255							
dst <addr6>	Destination IPv6 prefix. IPv6 address prefix.	string	Maximum length: 79							
dst-negate	Enable/disable negating destination address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable destination address negation.</td></tr><tr><td><i>disable</i></td><td>Disable destination address negation.</td></tr></table>	Option	Description	<i>enable</i>	Enable destination address negation.	<i>disable</i>	Disable destination address negation.			
Option	Description									
<i>enable</i>	Enable destination address negation.									
<i>disable</i>	Disable destination address negation.									
dstaddr <name>	Destination address name. Address/group name.	string	Maximum length: 79							
end-port	End destination port number (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	65535						
end-source-port	End source port number (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	65535						
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::						
groups <name>	List of user groups. Group name.	string	Maximum length: 79							
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79							
input-device-negate	Enable/disable negation of input device match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negation of input device match.</td></tr><tr><td><i>disable</i></td><td>Disable negation of input device match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negation of input device match.	<i>disable</i>	Disable negation of input device match.			
Option	Description									
<i>enable</i>	Enable negation of input device match.									
<i>disable</i>	Disable negation of input device match.									

Parameter	Description	Type	Size	Default						
internet-service-custom <name>	Custom Destination Internet Service name. Custom Destination Internet Service name.	string	Maximum length: 79							
internet-service-id <id>	Destination Internet Service ID. Destination Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295							
output-device	Outgoing interface name.	string	Maximum length: 35							
protocol	Protocol number (0 - 255).	integer	Minimum value: 0 Maximum value: 255							
seq-num	Sequence number(1-65535).	integer	Minimum value: 0 Maximum value: 65535							
src <addr6>	Source IPv6 prefix. IPv6 address prefix.	string	Maximum length: 79							
src-negate	Enable/disable negating source address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source address negation.</td></tr><tr><td>disable</td><td>Disable source address negation.</td></tr></table>				Option	Description	enable	Enable source address negation.	disable	Disable source address negation.
Option	Description									
enable	Enable source address negation.									
disable	Disable source address negation.									
srcaddr <name>	Source address name. Address/group name.	string	Maximum length: 79							
start-port	Start destination port number (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535							
start-source-port	Start source port number (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable this policy route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this policy route.</td></tr><tr><td>disable</td><td>Disable this policy route.</td></tr></table>				Option	Description	enable	Enable this policy route.	disable	Disable this policy route.
Option	Description									
enable	Enable this policy route.									
disable	Disable this policy route.									
tos	Type of service bit pattern.	user	Not Specified							

Parameter	Description	Type	Size	Default
tos-mask	Type of service evaluated bits.	user	Not Specified	
users <name>	List of users. User name.	string	Maximum length: 79	

config router prefix-list

Configure IPv4 prefix lists.

```

config router prefix-list
  Description: Configure IPv4 prefix lists.
  edit <name>
    set comments {string}
    config rule
      Description: IPv4 prefix list rule.
      edit <id>
        set action [permit|deny]
        set ge {integer}
        set le {integer}
        set prefix {user}
      next
    end
  next
end

```

config router prefix-list

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny this IP address and netmask prefix.	option	-	permit
	Option	Description		
	<i>permit</i>	Allow or permit packets that match this rule.		
	<i>deny</i>	Deny packets that match this rule.		

Parameter	Description	Type	Size	Default
ge	Minimum prefix length to be matched (0 - 32).	integer	Minimum value: 0 Maximum value: 32	
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	
le	Maximum prefix length to be matched (0 - 32).	integer	Minimum value: 0 Maximum value: 32	
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	0.0.0.0 0.0.0.0

config router prefix-list6

Configure IPv6 prefix lists.

```

config router prefix-list6
  Description: Configure IPv6 prefix lists.
  edit <name>
    set comments {string}
    config rule
      Description: IPv6 prefix list rule.
      edit <id>
        set action [permit|deny]
        set flags {integer}
        set ge {integer}
        set le {integer}
        set prefix6 {user}
      next
    end
  next
end

```

config router prefix-list6

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny packets that match this rule.	option	-	permit
	Option	Description		
	permit	Allow or permit packets that match this rule.		
	deny	Deny packets that match this rule.		
flags	Flags. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
ge	Minimum prefix length to be matched (0 - 128).	integer	Minimum value: 0 0 Maximum value: 128	
id	Rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
le	Maximum prefix length to be matched (0 - 128).	integer	Minimum value: 0 0 Maximum value: 128	
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	

config router rip

Configure RIP.

```
config router rip
  Description: Configure RIP.
  set default-information-originate [enable|disable]
  set default-metric {integer}
  config distance
    Description: Distance.
    edit <id>
      set access-list {string}
      set distance {integer}
      set prefix {ipv4-classnet-any}
    next
  end
  config distribute-list
    Description: Distribute list.
    edit <id>
```

```

        set direction [in|out]
        set interface {string}
        set listname {string}
        set status [enable|disable]
    next
end
set garbage-timer {integer}
config interface
    Description: RIP interface configuration.
    edit <name>
        set auth-keychain {string}
        set auth-mode [none|text|...]
        set auth-string {password}
        set flags {integer}
        set receive-version {option1}, {option2}, ...
        set send-version {option1}, {option2}, ...
        set send-version2-broadcast [disable|enable]
        set split-horizon [poisoned|regular]
        set split-horizon-status [enable|disable]
    next
end
set max-out-metric {integer}
config neighbor
    Description: Neighbor.
    edit <id>
        set ip {ipv4-address}
    next
end
config network
    Description: Network.
    edit <id>
        set prefix {ipv4-classnet}
    next
end
config offset-list
    Description: Offset list.
    edit <id>
        set access-list {string}
        set direction [in|out]
        set interface {string}
        set offset {integer}
        set status [enable|disable]
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration. Read-only.
    edit <name>
        set metric {integer}
        set routemap {string}
        set status [enable|disable]
    next

```

```

end
set timeout-timer {integer}
set update-timer {integer}
set version [1|2]
end

```

config router rip

Parameter	Description	Type	Size	Default						
default-information-originate	Enable/disable generation of default route.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16	1						
garbage-timer	Garbage timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	120						
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15	0						
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79							
timeout-timer	Timeout timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	180						
update-timer	Update timer in seconds.	integer	Minimum value: 1 Maximum value: 2147483647	30						

Parameter	Description	Type	Size	Default
version	RIP version.	option	-	2
	Option	Description		
	1	Version 1.		
	2	Version 2.		

config distance

Parameter	Description	Type	Size	Default
access-list	Access list for route destination.	string	Maximum length: 35	
distance	Distance (1 - 255).	integer	Minimum value: 1 Maximum value: 255	0
id	Distance ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Distance prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0

config distribute-list

Parameter	Description	Type	Size	Default						
direction	Distribute list direction.	option	-	out						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></table>				Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.
	Option	Description								
	<i>in</i>	Filter incoming packets.								
<i>out</i>	Filter outgoing packets.									
id	Distribute list ID.	integer	Minimum value: 0 Maximum value: 4294967295							
interface	Distribute list interface name.	string	Maximum length: 15							
listname	Distribute access/prefix list name.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config interface

Parameter	Description	Type	Size	Default
auth-keychain	Authentication key-chain name.	string	Maximum length: 35	
auth-mode	Authentication mode.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>text</i>	Text.		
	<i>md5</i>	MD5.		
auth-string	Authentication string/password.	password	Not Specified	
flags	Flags. Read-only.	integer	Minimum value: 0 Maximum value: 255	8
name	Interface name.	string	Maximum length: 35	
receive-version	Receive version.	option	-	
	Option	Description		
	<i>1</i>	Version 1.		
	<i>2</i>	Version 2.		
send-version	Send version.	option	-	
	Option	Description		
	<i>1</i>	Version 1.		
	<i>2</i>	Version 2.		

Parameter	Description	Type	Size	Default						
send-version2-broadcast	Enable/disable broadcast version 1 compatible packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable broadcasting.</td></tr><tr><td><i>enable</i></td><td>Enable broadcasting.</td></tr></table>	Option	Description	<i>disable</i>	Disable broadcasting.	<i>enable</i>	Enable broadcasting.			
Option	Description									
<i>disable</i>	Disable broadcasting.									
<i>enable</i>	Enable broadcasting.									
split-horizon	Enable/disable split horizon.	option	-	poisoned						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>poisoned</i></td><td>Poisoned.</td></tr><tr><td><i>regular</i></td><td>Regular.</td></tr></table>	Option	Description	<i>poisoned</i>	Poisoned.	<i>regular</i>	Regular.			
Option	Description									
<i>poisoned</i>	Poisoned.									
<i>regular</i>	Regular.									
split-horizon-status	Enable/disable split horizon.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config neighbor

Parameter	Description	Type	Size	Default
id	Neighbor entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
ip	IP address.	ipv4-address	Not Specified	0.0.0.0

config network

Parameter	Description	Type	Size	Default
id	Network entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config offset-list

Parameter	Description	Type	Size	Default
access-list	Access list name.	string	Maximum length: 35	
direction	Offset list direction.	option	-	out
	Option	Description		
	in	Filter incoming packets.		
	out	Filter outgoing packets.		
id	Offset-list ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
interface	Interface name.	string	Maximum length: 15	
offset	Offset.	integer	Minimum value: 0 1 Maximum value: 16	
status	Status.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

config redistribute

Parameter	Description	Type	Size	Default
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16	0
name	Redistribute name.	string	Maximum length: 35	
route-map	Route map name.	string	Maximum length: 35	
status	Status.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config router ripng

Configure RIPng.

```

config router ripng
    Description: Configure RIPng.
    config aggregate-address
        Description: Aggregate address.
        edit <id>
            set prefix6 {ipv6-prefix}
        next
    end
    set default-information-originate [enable|disable]
    set default-metric {integer}
    config distance
        Description: Distance.
        edit <id>
            set access-list6 {string}
            set distance {integer}
            set prefix6 {ipv6-prefix}
        next
    end
    config distribute-list
        Description: Distribute list.
        edit <id>
            set direction [in|out]
            set interface {string}
            set listname {string}
            set status [enable|disable]
        next
    end
    set garbage-timer {integer}
    config interface
        Description: RIPng interface configuration.
        edit <name>
            set flags {integer}
            set split-horizon [poisoned|regular]
            set split-horizon-status [enable|disable]
        next
    end
    set max-out-metric {integer}
    config neighbor

```

```

    Description: Neighbor.
    edit <id>
        set interface {string}
        set ip6 {ipv6-address}
    next
end
config network
    Description: Network.
    edit <id>
        set prefix {ipv6-prefix}
    next
end
config offset-list
    Description: Offset list.
    edit <id>
        set access-list6 {string}
        set direction [in|out]
        set interface {string}
        set offset {integer}
        set status [enable|disable]
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration. Read-only.
    edit <name>
        set metric {integer}
        set routemap {string}
        set status [enable|disable]
    next
end
set timeout-timer {integer}
set update-timer {integer}
end

```

config router ripng

Parameter	Description	Type	Size	Default
default-information-originate	Enable/disable generation of default route.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16	1
garbage-timer	Garbage timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	120
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15	0
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79	
timeout-timer	Timeout timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	180
update-timer	Update timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	30

config aggregate-address

Parameter	Description	Type	Size	Default
id	Aggregate address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	Aggregate address prefix.	ipv6-prefix	Not Specified	::/0

config distance

Parameter	Description	Type	Size	Default
access-list6	Access list for route destination.	string	Maximum length: 35	
distance	Distance (1 - 255).	integer	Minimum value: 1 Maximum value: 255	0
id	Distance ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	Distance prefix6.	ipv6-prefix	Not Specified	::/0

config distribute-list

Parameter	Description	Type	Size	Default
direction	Distribute list direction.	option	-	out
	Option	Description		
	<i>in</i>	Filter incoming packets.		
	<i>out</i>	Filter outgoing packets.		
id	Distribute list ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
interface	Distribute list interface name.	string	Maximum length: 15	
listname	Distribute access/prefix list name.	string	Maximum length: 35	
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config interface

Parameter	Description	Type	Size	Default						
flags	Flags. Read-only.	integer	Minimum value: 0 Maximum value: 255	8						
name	Interface name.	string	Maximum length: 35							
split-horizon	Enable/disable split horizon.	option	-	poisoned						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>poisoned</i></td><td>Poisoned.</td></tr><tr><td><i>regular</i></td><td>Regular.</td></tr></table>				Option	Description	<i>poisoned</i>	Poisoned.	<i>regular</i>	Regular.
Option	Description									
<i>poisoned</i>	Poisoned.									
<i>regular</i>	Regular.									
split-horizon-status	Enable/disable split horizon.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config neighbor

Parameter	Description	Type	Size	Default
id	Neighbor entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface name.	string	Maximum length: 15	
ip6	IPv6 link-local address.	ipv6-address	Not Specified	::

config network

Parameter	Description	Type	Size	Default
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
prefix	Network IPv6 link-local prefix.	ipv6-prefix	Not Specified	::/0

config offset-list

Parameter	Description	Type	Size	Default
access-list6	IPv6 access list name.	string	Maximum length: 35	
direction	Offset list direction.	option	-	out
	Option	Description		
	<i>in</i>	Filter incoming packets.		
	<i>out</i>	Filter outgoing packets.		
id	Offset-list ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
interface	Interface name.	string	Maximum length: 15	
offset	Offset.	integer	Minimum value: 0 1 Maximum value: 16	
status	Status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config redistribute

Parameter	Description	Type	Size	Default
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16	0
name	Redistribute name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
routemap	Route map name.	string	Maximum length: 35	
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config router route-map

Configure route maps.

```

config router route-map
  Description: Configure route maps.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set match-as-path {string}
        set match-community {string}
        set match-community-exact [enable|disable]
        set match-extcommunity {string}
        set match-extcommunity-exact [enable|disable]
        set match-interface {string}
        set match-ip-address {string}
        set match-ip-nexthop {string}
        set match-ip6-address {string}
        set match-ip6-nexthop {string}
        set match-metric {integer}
        set match-origin [none|egp|...]
        set match-route-type [external-type1|external-type2|...]
        set match-tag {integer}
        set match-vrf {integer}
        set set-aggregator-as {integer}
        set set-aggregator-ip {ipv4-address-any}
        set set-aspath <as1>, <as2>, ...
        set set-aspath-action [prepend|replace]
        set set-atomic-aggregate [enable|disable]
        set set-community <community1>, <community2>, ...
        set set-community-additive [enable|disable]
        set set-community-delete {string}
        set set-dampening-max-suppress {integer}
        set set-dampening-reachability-half-life {integer}
        set set-dampening-reuse {integer}

```

```

        set set-dampening-suppress {integer}
        set set-dampening-unreachability-half-life {integer}
        set set-extcommunity-rt <community1>, <community2>, ...
        set set-extcommunity-soo <community1>, <community2>, ...
        set set-ip-nexthop {ipv4-address}
        set set-ip-prefsrc {ipv4-address}
        set set-ip6-nexthop {ipv6-address}
        set set-ip6-nexthop-local {ipv6-address}
        set set-local-preference {integer}
        set set-metric {integer}
        set set-metric-type [external-type1|external-type2|...]
        set set-origin [none|egp|...]
        set set-originator-id {ipv4-address-any}
        set set-priority {integer}
        set set-route-tag {integer}
        set set-tag {integer}
        set set-vpnv4-nexthop {ipv4-address}
        set set-vpnv6-nexthop {ipv6-address}
        set set-vpnv6-nexthop-local {ipv6-address}
        set set-weight {integer}
    next
end
next
end

```

config router route-map

Parameter	Description	Type	Size	Default
comments	Optional comments.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

config rule

Parameter	Description	Type	Size	Default						
action	Action.	option	-	permit						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>permit</i></td><td>Permit.</td></tr><tr><td><i>deny</i></td><td>Deny.</td></tr></table>	Option	Description	<i>permit</i>	Permit.	<i>deny</i>	Deny.			
Option	Description									
<i>permit</i>	Permit.									
<i>deny</i>	Deny.									

Parameter	Description	Type	Size	Default						
id	Rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
match-as-path	Match BGP AS path list.	string	Maximum length: 35							
match-community	Match BGP community list.	string	Maximum length: 35							
match-community-exact	Enable/disable exact matching of communities.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable exact matching of communities.</td></tr><tr><td>disable</td><td>Disable exact matching of communities.</td></tr></table>				Option	Description	enable	Enable exact matching of communities.	disable	Disable exact matching of communities.
	Option	Description								
	enable	Enable exact matching of communities.								
disable	Disable exact matching of communities.									
match-extcommunity	Match BGP extended community list.	string	Maximum length: 35							
match-extcommunity-exact	Enable/disable exact matching of extended communities.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable exact matching of extended communities.</td></tr><tr><td>disable</td><td>Disable exact matching of extended communities.</td></tr></table>				Option	Description	enable	Enable exact matching of extended communities.	disable	Disable exact matching of extended communities.
	Option	Description								
	enable	Enable exact matching of extended communities.								
disable	Disable exact matching of extended communities.									
match-interface	Match interface configuration.	string	Maximum length: 15							
match-ip-address	Match IP address permitted by access-list or prefix-list.	string	Maximum length: 35							
match-ip-nexthop	Match next hop IP address passed by access-list or prefix-list.	string	Maximum length: 35							
match-ip6-address	Match IPv6 address permitted by access-list6 or prefix-list6.	string	Maximum length: 35							
match-ip6-nexthop	Match next hop IPv6 address passed by access-list6 or prefix-list6.	string	Maximum length: 35							
match-metric	Match metric for redistribute routes.	integer	Minimum value: 0 0 Maximum value: 4294967295							

Parameter	Description	Type	Size	Default										
match-origin	Match BGP origin code.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>None.</td></tr><tr><td>egp</td><td>Remote EGP.</td></tr><tr><td>igp</td><td>Local IGP.</td></tr><tr><td>incomplete</td><td>Unknown heritage.</td></tr></table>	Option	Description	none	None.	egp	Remote EGP.	igp	Local IGP.	incomplete	Unknown heritage.			
	Option	Description												
	none	None.												
	egp	Remote EGP.												
	igp	Local IGP.												
incomplete	Unknown heritage.													
match-route-type	Match route type.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>external-type1</td><td>External type 1.</td></tr><tr><td>external-type2</td><td>External type 2.</td></tr><tr><td>none</td><td>No type specified.</td></tr></table>	Option	Description	external-type1	External type 1.	external-type2	External type 2.	none	No type specified.					
	Option	Description												
	external-type1	External type 1.												
	external-type2	External type 2.												
	none	No type specified.												
match-tag	Match tag.	integer	Minimum value: 0 Maximum value: 4294967295											
match-vrf	Match VRF ID.	integer	Minimum value: 0 Maximum value: 511											
set-aggregator-as	BGP aggregator AS.	integer	Minimum value: 0 Maximum value: 4294967295	0										
set-aggregator-ip	BGP aggregator IP.	ipv4-address-any	Not Specified	0.0.0.0										
set-aspath <as>	Prepend BGP AS path attribute. AS number (0 - 4294967295). Use quotes for repeating numbers, For example, "1 1 2".	string	Maximum length: 79											
set-aspath-action	Specify preferred action of set-aspath.	option	-	prepend										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>prepend</td><td>Prepend.</td></tr><tr><td>replace</td><td>Replace.</td></tr></table>	Option	Description	prepend	Prepend.	replace	Replace.							
	Option	Description												
	prepend	Prepend.												
replace	Replace.													

Parameter	Description	Type	Size	Default
set-atomic-aggregate	Enable/disable BGP atomic aggregate attribute.	option	-	disable
	Option	Description		
	enable	Enable BGP atomic aggregate attribute.		
	disable	Disable BGP atomic aggregate attribute.		
set-community <community>	BGP community attribute. Attribute: AA AA:NN internet local-AS no-advertise no-export (exact match required for well known communities).	string	Maximum length: 79	
set-community-additive	Enable/disable adding set-community to existing community.	option	-	disable
	Option	Description		
	enable	Enable adding set-community to existing community.		
	disable	Disable adding set-community to existing community.		
set-community-delete	Delete communities matching community list.	string	Maximum length: 35	
set-dampening-max-suppress	Maximum duration to suppress a route (1 - 255 min, 0 = unset).	integer	Minimum value: 0 0 Maximum value: 255	
set-dampening-reachability-half-life	Reachability half-life time for the penalty (1 - 45 min, 0 = unset).	integer	Minimum value: 0 0 Maximum value: 45	
set-dampening-reuse	Value to start reusing a route (1 - 20000, 0 = unset).	integer	Minimum value: 0 0 Maximum value: 20000	
set-dampening-suppress	Value to start suppressing a route (1 - 20000, 0 = unset).	integer	Minimum value: 0 0 Maximum value: 20000	
set-dampening-unreachability-half-life	Unreachability Half-life time for the penalty (1 - 45 min, 0 = unset).	integer	Minimum value: 0 0 Maximum value: 45	
set-extcommunity-rt <community>	Route Target extended community. AA:NN.	string	Maximum length: 79	
set-extcommunity-soo <community>	Site-of-Origin extended community. Community (format = AA:NN).	string	Maximum length: 79	

Parameter	Description	Type	Size	Default										
set-ip-nexthop	IP address of next hop.	ipv4-address	Not Specified											
set-ip-prefsrc	IP address of preferred source.	ipv4-address	Not Specified											
set-ip6-nexthop	IPv6 global address of next hop.	ipv6-address	Not Specified											
set-ip6-nexthop-local	IPv6 local address of next hop.	ipv6-address	Not Specified											
set-local-preference	BGP local preference path attribute.	integer	Minimum value: 0 Maximum value: 4294967295											
set-metric	Metric value.	integer	Minimum value: 0 Maximum value: 4294967295											
set-metric-type	Metric type.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>external-type1</i></td><td>External type 1.</td></tr><tr><td><i>external-type2</i></td><td>External type 2.</td></tr><tr><td><i>none</i></td><td>No type specified.</td></tr></table>	Option	Description	<i>external-type1</i>	External type 1.	<i>external-type2</i>	External type 2.	<i>none</i>	No type specified.					
Option	Description													
<i>external-type1</i>	External type 1.													
<i>external-type2</i>	External type 2.													
<i>none</i>	No type specified.													
set-origin	BGP origin code.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>egp</i></td><td>Remote EGP.</td></tr><tr><td><i>igp</i></td><td>Local IGP.</td></tr><tr><td><i>incomplete</i></td><td>Unknown heritage.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>egp</i>	Remote EGP.	<i>igp</i>	Local IGP.	<i>incomplete</i>	Unknown heritage.			
Option	Description													
<i>none</i>	None.													
<i>egp</i>	Remote EGP.													
<i>igp</i>	Local IGP.													
<i>incomplete</i>	Unknown heritage.													
set-originator-id	BGP originator ID attribute.	ipv4-address-any	Not Specified											
set-priority	Priority for routing table.	integer	Minimum value: 1 Maximum value: 65535											

Parameter	Description	Type	Size	Default
set-route-tag	Route tag for routing table.	integer	Minimum value: 0 Maximum value: 4294967295	
set-tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	
set-vpnv4-nexthop	IP address of VPNv4 next-hop.	ipv4-address	Not Specified	
set-vpnv6-nexthop	IPv6 global address of VPNv6 next-hop.	ipv6-address	Not Specified	
set-vpnv6-nexthop-local	IPv6 link-local address of VPNv6 next-hop.	ipv6-address	Not Specified	
set-weight	BGP weight for routing table.	integer	Minimum value: 0 Maximum value: 4294967295	

config router setting

Configure router settings.

```

config router setting
    Description: Configure router settings.
    set hostname {string}
    set kernel-route-distance {integer}
    set show-filter {string}
end

```

config router setting

Parameter	Description	Type	Size	Default
hostname	Hostname for this virtual domain router.	string	Maximum length: 14	
kernel-route-distance	Administrative distance for routes learned from kernel (0 - 255).	integer	Minimum value: 0 Maximum value: 255	255
show-filter	Prefix-list as filter for showing routes.	string	Maximum length: 35	

config router static

Configure IPv4 static routing tables.

```
config router static
  Description: Configure IPv4 static routing tables.
  edit <seq-num>
    set bfd [enable|disable]
    set blackhole [enable|disable]
    set comment {var-string}
    set device {string}
    set distance {integer}
    set dst {ipv4-classnet}
    set dstaddr {string}
    set dynamic-gateway [enable|disable]
    set gateway {ipv4-address}
    set internet-service {integer}
    set internet-service-custom {string}
    set link-monitor-exempt [enable|disable]
    set preferred-source {ipv4-address}
    set priority {integer}
    set sdwan-zone <name1>, <name2>, ...
    set src {ipv4-classnet}
    set status [enable|disable]
    set tag {integer}
    set vrf {integer}
    set weight {integer}
  next
end
```

config router static

Parameter	Description	Type	Size	Default						
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>disable</i></td><td>Disable Bidirectional Forwarding Detection (BFD).</td></tr></table>	Option	Description	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).			
Option	Description									
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).									
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).									
blackhole	Enable/disable black hole.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable black hole.</td></tr><tr><td><i>disable</i></td><td>Disable black hole.</td></tr></table>	Option	Description	<i>enable</i>	Enable black hole.	<i>disable</i>	Disable black hole.			
Option	Description									
<i>enable</i>	Enable black hole.									
<i>disable</i>	Disable black hole.									

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
device	Gateway out interface or tunnel.	string	Maximum length: 35							
distance	Administrative distance (1 - 255).	integer	Minimum value: 1 Maximum value: 255	10						
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
dstaddr	Name of firewall address or address group.	string	Maximum length: 79							
dynamic-gateway	Enable use of dynamic gateway retrieved from a DHCP or PPP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dynamic gateway.</td></tr><tr><td>disable</td><td>Disable dynamic gateway.</td></tr></table>				Option	Description	enable	Enable dynamic gateway.	disable	Disable dynamic gateway.
Option	Description									
enable	Enable dynamic gateway.									
disable	Disable dynamic gateway.									
gateway	Gateway IP for this route.	ipv4-address	Not Specified	0.0.0.0						
internet-service	Application ID in the Internet service database.	integer	Minimum value: 0 Maximum value: 4294967295	0						
internet-service-custom	Application name in the Internet service custom database.	string	Maximum length: 64							
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Keep this static route when link monitor or health check is down.</td></tr><tr><td>disable</td><td>Withdraw this static route when link monitor or health check is down. (default)</td></tr></table>				Option	Description	enable	Keep this static route when link monitor or health check is down.	disable	Withdraw this static route when link monitor or health check is down. (default)
Option	Description									
enable	Keep this static route when link monitor or health check is down.									
disable	Withdraw this static route when link monitor or health check is down. (default)									
preferred-source	Preferred source IP for this route.	ipv4-address	Not Specified	0.0.0.0						
priority	Administrative priority (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	1						

Parameter	Description	Type	Size	Default
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79	
seq-num	Sequence number.	integer	Minimum value: 0 0 Maximum value: 4294967295	
src	Source prefix for this route.	ipv4- classnet	Not Specified	0.0.0.0 0.0.0.0
status	Enable/disable this static route.	option	-	enable
	Option Description			
	enable Enable static route.			
	disable Disable static route.			
tag	Route tag.	integer	Minimum value: 0 0 Maximum value: 4294967295	
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 0 Maximum value: 511	unspecified
weight	Administrative weight (0 - 255).	integer	Minimum value: 0 0 Maximum value: 255	

config router static6

Configure IPv6 static routing tables.

```

config router static6
  Description: Configure IPv6 static routing tables.
  edit <seq-num>
    set bfd [enable|disable]
    set blackhole [enable|disable]
    set comment {var-string}
    set device {string}
    set devindex {integer}
    set distance {integer}
    set dst {ipv6-network}
    set dstaddr {string}
    set dynamic-gateway [enable|disable]
    set gateway {ipv6-address}
    set link-monitor-exempt [enable|disable]

```

```

    set priority {integer}
    set sdwan-zone <name1>, <name2>, ...
    set status [enable|disable]
    set tag {integer}
    set vrf {integer}
    set weight {integer}
  next
end

```

config router static6

Parameter	Description	Type	Size	Default
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).		
	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).		
blackhole	Enable/disable black hole.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable black hole.		
	<i>disable</i>	Disable black hole.		
comment	Optional comments.	var-string	Maximum length: 255	
device	Gateway out interface or tunnel.	string	Maximum length: 35	
devindex	Device index (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	
distance	Administrative distance (1 - 255).	integer	Minimum value: 1 Maximum value: 255	
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0
dstaddr	Name of firewall address or address group.	string	Maximum length: 79	
dynamic-gateway	Enable use of dynamic gateway retrieved from Router Advertisement (RA).	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic gateway.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic gateway.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic gateway.	<i>disable</i>	Disable dynamic gateway.			
	Option	Description								
	<i>enable</i>	Enable dynamic gateway.								
<i>disable</i>	Disable dynamic gateway.									
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::						
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep this static route when link monitor or health check is down.</td></tr><tr><td><i>disable</i></td><td>Withdraw this static route when link monitor or health check is down. (default)</td></tr></table>	Option	Description	<i>enable</i>	Keep this static route when link monitor or health check is down.	<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)			
	Option	Description								
	<i>enable</i>	Keep this static route when link monitor or health check is down.								
<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)									
priority	Administrative priority (1 - 65535).	integer	Minimum value: 1024 Maximum value: 65535							
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79							
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295							
status	Enable/disable this static route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable static route.</td></tr><tr><td><i>disable</i></td><td>Disable static route.</td></tr></table>	Option	Description	<i>enable</i>	Enable static route.	<i>disable</i>	Disable static route.			
	Option	Description								
	<i>enable</i>	Enable static route.								
<i>disable</i>	Disable static route.									
tag	Route tag.	integer	Minimum value: 0 Maximum value: 4294967295							
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 511	unspecified						
weight	Administrative weight (0 - 255).	integer	Minimum value: 0 Maximum value: 255							

rule

This section includes syntax for the following commands:

- [config rule fmwp on page 1157](#)
- [config rule iotd on page 1159](#)
- [config rule otdt on page 1161](#)
- [config rule otvp on page 1163](#)

config rule fmwp

Show FMWP signatures. Read-only.

```
config rule fmwp
  Description: Show FMWP signatures. Read-only.
  edit <name>
    set action [pass|block]
    set application {user}
    set date {integer}
    set group {string}
    set location {user}
    set log [disable|enable]
    set log-packet [disable|enable]
    config metadata
      Description: Meta data. Read-only.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
    set os {user}
    set rev {integer}
    set rule-id {integer}
    set service {user}
    set severity {user}
  next
end
```

config rule fmwp

Parameter	Description	Type	Size	Default
action	Action. Read-only.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
application	Vulnerable applications. Read-only.	user	Not Specified	
date	Date. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
group	Group. Read-only.	string	Maximum length: 63	
location	Vulnerable location. Read-only.	user	Not Specified	
log	Enable/disable logging. Read-only.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
log-packet	Enable/disable packet logging. Read-only.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable packet logging.		
	<i>enable</i>	Enable packet logging.		
name	Rule name.	string	Maximum length: 63	
os	Vulnerable operation systems. Read-only.	user	Not Specified	
rev	Revision. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
rule-id	Rule ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
service	Vulnerable service. Read-only.	user	Not Specified	
severity	Severity. Read-only.	user	Not Specified	

config metadata

Parameter	Description	Type	Size	Default
id	ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
metaid	Meta ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
valueid	Value ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

config rule iotd

Show IOT detection signatures. Read-only.

```
config rule iotd
  Description: Show IOT detection signatures. Read-only.
  edit <name>
    set behavior {user}
    set category {integer}
    set id {integer}
    config metadata
      Description: Meta data. Read-only.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
  end
  config parameters
    Description: Application parameters. Read-only.
    edit <name>
      set default value {string}
    next
  end
  set popularity {integer}
  set protocol {user}
  set risk {integer}
  set technology {user}
  set vendor {user}
  set weight {integer}
next
end
```

config rule iotd

Parameter	Description	Type	Size	Default
behavior	Application behavior. Read-only.	user	Not Specified	
category	Application category ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
id	Application ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
name	Application name.	string	Maximum length: 63	
popularity	Application popularity. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	
protocol	Application protocol. Read-only.	user	Not Specified	
risk	Application risk. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	
technology	Application technology. Read-only.	user	Not Specified	
vendor	Application vendor. Read-only.	user	Not Specified	
weight	Application weight. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	

config metadata

Parameter	Description	Type	Size	Default
id	ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
metaid	Meta ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
valueid	Value ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

config parameters

Parameter	Description	Type	Size	Default
default value	Parameter default value. Read-only.	string	Maximum length: 199	
name	Parameter name. Read-only.	string	Maximum length: 31	

config rule otdt

Show OT detection signatures. Read-only.

```

config rule otdt
  Description: Show OT detection signatures. Read-only.
  edit <name>
    set behavior {user}
    set category {integer}
    set id {integer}
    config metadata
      Description: Meta data. Read-only.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
  config parameters
    Description: Application parameters. Read-only.
    edit <name>
      set default value {string}
    next
  end
  set popularity {integer}
  set protocol {user}
  set risk {integer}
  set technology {user}
  set vendor {user}
  set weight {integer}
next
end

```

config rule otdt

Parameter	Description	Type	Size	Default
behavior	Application behavior. Read-only.	user	Not Specified	
category	Application category ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
id	Application ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
name	Application name.	string	Maximum length: 63	
popularity	Application popularity. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	
protocol	Application protocol. Read-only.	user	Not Specified	
risk	Application risk. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	
technology	Application technology. Read-only.	user	Not Specified	
vendor	Application vendor. Read-only.	user	Not Specified	
weight	Application weight. Read-only.	integer	Minimum value: 0 0 Maximum value: 255	

config metadata

Parameter	Description	Type	Size	Default
id	ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
metaid	Meta ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
valueid	Value ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

config parameters

Parameter	Description	Type	Size	Default
default value	Parameter default value. Read-only.	string	Maximum length: 199	
name	Parameter name. Read-only.	string	Maximum length: 31	

config rule otp

Show OT patch signatures. Read-only.

```

config rule otp
  Description: Show OT patch signatures. Read-only.
  edit <name>
    set action [pass|block]
    set application {user}
    set date {integer}
    set group {string}
    set location {user}
    set log [disable|enable]
    set log-packet [disable|enable]
    config metadata
      Description: Meta data. Read-only.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
    set os {user}
    set rev {integer}
    set rule-id {integer}
    set service {user}
    set severity {user}
  next
end

```

config rule otvp

Parameter	Description	Type	Size	Default						
action	Action. Read-only.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Pass or allow matching traffic.</td></tr><tr><td><i>block</i></td><td>Block or drop matching traffic.</td></tr></table>				Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.
	Option	Description								
	<i>pass</i>	Pass or allow matching traffic.								
<i>block</i>	Block or drop matching traffic.									
application	Vulnerable applications. Read-only.	user	Not Specified							
date	Date. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							
group	Group. Read-only.	string	Maximum length: 63							
location	Vulnerable location. Read-only.	user	Not Specified							
log	Enable/disable logging. Read-only.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr></table>				Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.
	Option	Description								
	<i>disable</i>	Disable logging.								
<i>enable</i>	Enable logging.									
log-packet	Enable/disable packet logging. Read-only.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet logging.</td></tr><tr><td><i>enable</i></td><td>Enable packet logging.</td></tr></table>				Option	Description	<i>disable</i>	Disable packet logging.	<i>enable</i>	Enable packet logging.
	Option	Description								
	<i>disable</i>	Disable packet logging.								
<i>enable</i>	Enable packet logging.									
name	Rule name.	string	Maximum length: 63							
os	Vulnerable operation systems. Read-only.	user	Not Specified							
rev	Revision. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							
rule-id	Rule ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							
service	Vulnerable service. Read-only.	user	Not Specified							

Parameter	Description	Type	Size	Default
severity	Severity. Read-only.	user	Not Specified	

config metadata

Parameter	Description	Type	Size	Default
id	ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
metaid	Meta ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
valueid	Value ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

sctp-filter

This section includes syntax for the following commands:

- [config sctp-filter profile on page 1166](#)

config sctp-filter profile

Configure SCTP filter profiles.

```
config sctp-filter profile
  Description: Configure SCTP filter profiles.
  edit <name>
    set comment {var-string}
    config ppid-filters
      Description: PPID filters list.
      edit <id>
        set action [pass|reset|...]
        set comment {var-string}
        set ppid {integer}
      next
    end
  next
end
```

config sctp-filter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Profile name.	string	Maximum length: 47	

config ppid-filters

Parameter	Description	Type	Size	Default
action	Action taken when PPID is matched.	option	-	reset

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Pass data chunk.</td></tr><tr><td><i>reset</i></td><td>Reset SCTP session.</td></tr><tr><td><i>replace</i></td><td>Replace data chunk.</td></tr></table>	Option	Description	<i>pass</i>	Pass data chunk.	<i>reset</i>	Reset SCTP session.	<i>replace</i>	Replace data chunk.			
	Option	Description										
	<i>pass</i>	Pass data chunk.										
	<i>reset</i>	Reset SCTP session.										
<i>replace</i>	Replace data chunk.											
comment	Comment.	var-string	Maximum length: 255									
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295									
ppid	Payload protocol identifier.	integer	Minimum value: 0 Maximum value: 4294967295									

ssh-filter

This section includes syntax for the following commands:

- [config ssh-filter profile on page 1168](#)

config ssh-filter profile



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure SSH filter profile.

```
config ssh-filter profile
  Description: Configure SSH filter profile.
  edit <name>
    set block {option1}, {option2}, ...
    set default-command-log [enable|disable]
    set log {option1}, {option2}, ...
    config shell-commands
      Description: SSH command filter.
      edit <id>
        set action [block|allow]
```



```

        set alert [enable|disable]
        set log [enable|disable]
        set pattern {string}
        set severity [low|medium|...]
        set type [simple|regex]
    next
end
next
end

```

config ssh-filter profile

Parameter	Description	Type	Size	Default																		
block	SSH blocking options.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>x11</i></td><td>X server forwarding.</td></tr><tr><td><i>shell</i></td><td>SSH shell.</td></tr><tr><td><i>exec</i></td><td>SSH execution.</td></tr><tr><td><i>port-forward</i></td><td>Port forwarding.</td></tr><tr><td><i>tun-forward</i></td><td>Tunnel forwarding.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr><tr><td><i>scp</i></td><td>SCP.</td></tr><tr><td><i>unknown</i></td><td>Unknown channel.</td></tr></table>	Option	Description	<i>x11</i>	X server forwarding.	<i>shell</i>	SSH shell.	<i>exec</i>	SSH execution.	<i>port-forward</i>	Port forwarding.	<i>tun-forward</i>	Tunnel forwarding.	<i>sftp</i>	SFTP.	<i>scp</i>	SCP.	<i>unknown</i>	Unknown channel.			
Option	Description																					
<i>x11</i>	X server forwarding.																					
<i>shell</i>	SSH shell.																					
<i>exec</i>	SSH execution.																					
<i>port-forward</i>	Port forwarding.																					
<i>tun-forward</i>	Tunnel forwarding.																					
<i>sftp</i>	SFTP.																					
<i>scp</i>	SCP.																					
<i>unknown</i>	Unknown channel.																					
default-command-log	Enable/disable logging unmatched shell commands.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable log unmatched shell commands.</td></tr><tr><td><i>disable</i></td><td>Disable log unmatched shell commands.</td></tr></table>	Option	Description	<i>enable</i>	Enable log unmatched shell commands.	<i>disable</i>	Disable log unmatched shell commands.															
Option	Description																					
<i>enable</i>	Enable log unmatched shell commands.																					
<i>disable</i>	Disable log unmatched shell commands.																					
log	SSH logging options.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>x11</i></td><td>X server forwarding.</td></tr><tr><td><i>shell</i></td><td>SSH shell.</td></tr><tr><td><i>exec</i></td><td>SSH execution.</td></tr></table>	Option	Description	<i>x11</i>	X server forwarding.	<i>shell</i>	SSH shell.	<i>exec</i>	SSH execution.													
Option	Description																					
<i>x11</i>	X server forwarding.																					
<i>shell</i>	SSH shell.																					
<i>exec</i>	SSH execution.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>port-forward</i>	Port forwarding.		
	<i>tun-forward</i>	Tunnel forwarding.		
	<i>sftp</i>	SFTP.		
	<i>scp</i>	SCP.		
	<i>unknown</i>	Unknown channel.		
name	SSH filter profile name.	string	Maximum length: 47	

config shell-commands

Parameter	Description	Type	Size	Default
action	Action to take for SSH shell command matches.	option	-	block
	Option	Description		
	<i>block</i>	Block the SSH shell command.		
	<i>allow</i>	Allow the SSH shell command.		
alert	Enable/disable alert.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable alert.		
	<i>disable</i>	Disable alert.		
id	Id.	integer	Minimum value: 0 0 Maximum value: 4294967295	
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		
pattern	SSH shell command pattern.	string	Maximum length: 128	
severity	Log severity.	option	-	medium

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>low</i>	Severity low.		
	<i>medium</i>	Severity medium.		
	<i>high</i>	Severity high.		
	<i>critical</i>	Severity critical.		
type	Matching type.	option	-	simple
	Option	Description		
	<i>simple</i>	Match single command.		
	<i>regex</i>	Match command line using regular expression.		

switch-controller

This section includes syntax for the following commands:

- [config switch-controller 802-1X-settings on page 1173](#)
- [config switch-controller acl group on page 1176](#)
- [config switch-controller acl ingress on page 1177](#)
- [config switch-controller auto-config custom on page 1179](#)
- [config switch-controller auto-config default on page 1181](#)
- [config switch-controller auto-config policy on page 1182](#)
- [config switch-controller custom-command on page 1184](#)
- [config switch-controller dsl policy on page 1185](#)
- [config switch-controller dynamic-port-policy on page 1188](#)
- [config switch-controller flow-tracking on page 1192](#)
- [config switch-controller fortilink-settings on page 1196](#)
- [config switch-controller global on page 1198](#)
- [config switch-controller igmp-snooping on page 1204](#)
- [config switch-controller initial-config template on page 1206](#)
- [config switch-controller initial-config vlans on page 1208](#)
- [config switch-controller lldp-profile on page 1210](#)
- [config switch-controller lldp-settings on page 1215](#)
- [config switch-controller location on page 1216](#)
- [config switch-controller mac-policy on page 1221](#)
- [config switch-controller managed-switch on page 1223](#)
- [config switch-controller network-monitor-settings on page 1266](#)
- [config switch-controller ptp interface-policy on page 1267](#)
- [config switch-controller ptp profile on page 1268](#)
- [config switch-controller qos dot1p-map on page 1270](#)
- [config switch-controller qos ip-dscp-map on page 1274](#)
- [config switch-controller qos qos-policy on page 1277](#)
- [config switch-controller qos queue-policy on page 1278](#)
- [config switch-controller quarantine on page 1281](#)
- [config switch-controller remote-log on page 1282](#)
- [config switch-controller security-policy 802-1X on page 1285](#)
- [config switch-controller security-policy local-access on page 1290](#)
- [config switch-controller sflow on page 1292](#)
- [config switch-controller snmp-community on page 1293](#)
- [config switch-controller snmp-sysinfo on page 1296](#)
- [config switch-controller snmp-trap-threshold on page 1297](#)
- [config switch-controller snmp-user on page 1299](#)

- [config switch-controller storm-control-policy on page 1303](#)
- [config switch-controller storm-control on page 1301](#)
- [config switch-controller stp-instance on page 1305](#)
- [config switch-controller stp-settings on page 1306](#)
- [config switch-controller switch-group on page 1308](#)
- [config switch-controller switch-interface-tag on page 1309](#)
- [config switch-controller switch-log on page 1310](#)
- [config switch-controller switch-profile on page 1311](#)
- [config switch-controller system on page 1313](#)
- [config switch-controller traffic-policy on page 1316](#)
- [config switch-controller traffic-sniffer on page 1318](#)
- [config switch-controller virtual-port-pool on page 1320](#)
- [config switch-controller vlan-policy on page 1321](#)

config switch-controller 802-1X-settings



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure global 802.1X settings.

```
config switch-controller 802-1X-settings
  Description: Configure global 802.1X settings.
  set link-down-auth [set-unauth|no-action]
  set mab-reauth [disable|enable]
```

```

set mac-called-station-delimiter [colon|hyphen|...]
set mac-calling-station-delimiter [colon|hyphen|...]
set mac-case [lowercase|uppercase]
set mac-password-delimiter [colon|hyphen|...]
set mac-username-delimiter [colon|hyphen|...]
set max-reauth-attempt {integer}
set reauth-period {integer}
set tx-period {integer}
end

```

config switch-controller 802-1X-settings

Parameter	Description	Type	Size	Default										
link-down-auth	Interface-reauthentication state to set if a link is down.	option	-	set-unauth										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>set-unauth</td><td>Interface set to unauth when down. Reauthentication is needed.</td></tr><tr><td>no-action</td><td>Interface reauthentication is not needed.</td></tr></table>	Option	Description	set-unauth	Interface set to unauth when down. Reauthentication is needed.	no-action	Interface reauthentication is not needed.							
Option	Description													
set-unauth	Interface set to unauth when down. Reauthentication is needed.													
no-action	Interface reauthentication is not needed.													
mab-reauth	Enable/disable MAB re-authentication.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable MAB re-authentication.</td></tr><tr><td>enable</td><td>Enable MAB re-authentication.</td></tr></table>	Option	Description	disable	Disable MAB re-authentication.	enable	Enable MAB re-authentication.							
Option	Description													
disable	Disable MAB re-authentication.													
enable	Enable MAB re-authentication.													
mac-called-station-delimiter	MAC called station delimiter (default = hyphen).	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>colon</td><td>Use colon as delimiter for called station.</td></tr><tr><td>hyphen</td><td>Use hyphen as delimiter for called station.</td></tr><tr><td>none</td><td>No delimiter for called station.</td></tr><tr><td>single-hyphen</td><td>Use single hyphen as delimiter for called station.</td></tr></table>	Option	Description	colon	Use colon as delimiter for called station.	hyphen	Use hyphen as delimiter for called station.	none	No delimiter for called station.	single-hyphen	Use single hyphen as delimiter for called station.			
Option	Description													
colon	Use colon as delimiter for called station.													
hyphen	Use hyphen as delimiter for called station.													
none	No delimiter for called station.													
single-hyphen	Use single hyphen as delimiter for called station.													
mac-calling-station-delimiter	MAC calling station delimiter (default = hyphen).	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>colon</td><td>Use colon as delimiter for calling station.</td></tr></table>	Option	Description	colon	Use colon as delimiter for calling station.									
Option	Description													
colon	Use colon as delimiter for calling station.													

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hyphen</td><td>Use hyphen as delimiter for calling station.</td></tr><tr><td>none</td><td>No delimiter for calling station.</td></tr><tr><td>single-hyphen</td><td>Use single hyphen as delimiter for calling station.</td></tr></table>	Option	Description	hyphen	Use hyphen as delimiter for calling station.	none	No delimiter for calling station.	single-hyphen	Use single hyphen as delimiter for calling station.					
Option	Description													
hyphen	Use hyphen as delimiter for calling station.													
none	No delimiter for calling station.													
single-hyphen	Use single hyphen as delimiter for calling station.													
mac-case	MAC case (default = lowercase).	option	-	lowercase										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>lowercase</td><td>Use lowercase MAC.</td></tr><tr><td>uppercase</td><td>Use uppercase MAC.</td></tr></table>	Option	Description	lowercase	Use lowercase MAC.	uppercase	Use uppercase MAC.							
Option	Description													
lowercase	Use lowercase MAC.													
uppercase	Use uppercase MAC.													
mac-password-delimiter	MAC authentication password delimiter (default = hyphen).	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>colon</td><td>Use colon as delimiter for MAC auth password.</td></tr><tr><td>hyphen</td><td>Use hyphen as delimiter for MAC auth password.</td></tr><tr><td>none</td><td>No delimiter for MAC auth password.</td></tr><tr><td>single-hyphen</td><td>Use single hyphen as delimiter for MAC auth password.</td></tr></table>	Option	Description	colon	Use colon as delimiter for MAC auth password.	hyphen	Use hyphen as delimiter for MAC auth password.	none	No delimiter for MAC auth password.	single-hyphen	Use single hyphen as delimiter for MAC auth password.			
Option	Description													
colon	Use colon as delimiter for MAC auth password.													
hyphen	Use hyphen as delimiter for MAC auth password.													
none	No delimiter for MAC auth password.													
single-hyphen	Use single hyphen as delimiter for MAC auth password.													
mac-username-delimiter	MAC authentication username delimiter (default = hyphen).	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>colon</td><td>Use colon as delimiter for MAC auth username.</td></tr><tr><td>hyphen</td><td>Use hyphen as delimiter for MAC auth username.</td></tr><tr><td>none</td><td>No delimiter for MAC auth username.</td></tr><tr><td>single-hyphen</td><td>Use single hyphen as delimiter for MAC auth username.</td></tr></table>	Option	Description	colon	Use colon as delimiter for MAC auth username.	hyphen	Use hyphen as delimiter for MAC auth username.	none	No delimiter for MAC auth username.	single-hyphen	Use single hyphen as delimiter for MAC auth username.			
Option	Description													
colon	Use colon as delimiter for MAC auth username.													
hyphen	Use hyphen as delimiter for MAC auth username.													
none	No delimiter for MAC auth username.													
single-hyphen	Use single hyphen as delimiter for MAC auth username.													
max-reauth-attempt	Maximum number of authentication attempts (0 - 15, default = 3).	integer	Minimum value: 0 Maximum value: 15	3										
reauth-period	Period of time to allow for reauthentication (1 - 1440 sec, default = 60, 0 = disable reauthentication).	integer	Minimum value: 0 Maximum value: 1440	60										

Parameter	Description	Type	Size	Default
tx-period	802.1X Tx period (seconds, default=30).	integer	Minimum value: 12 Maximum value: 60	30

config switch-controller acl group



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure ACL groups to be applied on managed FortiSwitch ports.

```
config switch-controller acl group
    Description: Configure ACL groups to be applied on managed FortiSwitch ports.
    edit <name>
        set ingress <id1>, <id2>, ...
    next
end
```


config switch-controller acl group

Parameter	Description	Type	Size	Default
ingress <id>	Configure ingress ACL policies in group. ACL ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Group name.	string	Maximum length: 63	

config switch-controller acl ingress



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure ingress ACL policies to be applied on managed FortiSwitch ports.

```
config switch-controller acl ingress
  Description: Configure ingress ACL policies to be applied on managed FortiSwitch ports.
  edit <id>
    config action
      Description: ACL actions.
      set count [enable|disable]
      set drop [enable|disable]
    end
```

```

config classifier
    Description: ACL classifiers.
    set dst-ip-prefix {ipv4-classnet}
    set dst-mac {mac-address}
    set src-ip-prefix {ipv4-classnet}
    set src-mac {mac-address}
    set vlan {integer}
end
set description {string}
next
end

```

config switch-controller acl ingress

Parameter	Description	Type	Size	Default
description	Description for the ACL policy.	string	Maximum length: 63	
id	ACL ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config action

Parameter	Description	Type	Size	Default						
count	Enable/disable count.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable count.</td></tr><tr><td><i>disable</i></td><td>Disable count.</td></tr></table>	Option	Description	<i>enable</i>	Enable count.	<i>disable</i>	Disable count.			
Option	Description									
<i>enable</i>	Enable count.									
<i>disable</i>	Disable count.									
drop	Enable/disable drop.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable drop.</td></tr><tr><td><i>disable</i></td><td>Disable drop.</td></tr></table>	Option	Description	<i>enable</i>	Enable drop.	<i>disable</i>	Disable drop.			
Option	Description									
<i>enable</i>	Enable drop.									
<i>disable</i>	Disable drop.									

config classifier

Parameter	Description	Type	Size	Default
dst-ip-prefix	Destination IP address to be matched.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
dst-mac	Destination MAC address to be matched.	mac-address	Not Specified	00:00:00:00:00:00
src-ip-prefix	Source IP address to be matched.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
src-mac	Source MAC address to be matched.	mac-address	Not Specified	00:00:00:00:00:00
vlan	VLAN ID to be matched.	integer	Minimum value: 1 Maximum value: 4094	0

config switch-controller auto-config custom



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Policies which can override the 'default' for specific ISL/ICL/FortiLink interface.

```
config switch-controller auto-config custom
    Description: Policies which can override the 'default' for specific ISL/ICL/FortiLink
    interface.
    edit <name>
        config switch-binding
            Description: Switch binding list.
            edit <switch-id>
                set policy {string}
            next
        end
    next
end
```

config switch-controller auto-config custom

Parameter	Description	Type	Size	Default
name	Auto-Config FortiLink or ISL/ICL interface name.	string	Maximum length: 15	

config switch-binding

Parameter	Description	Type	Size	Default
policy	Custom auto-config policy.	string	Maximum length: 63	default
switch-id	Switch name.	string	Maximum length: 16	

config switch-controller auto-config default



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Policies which are applied automatically to all ISL/ICL/FortiLink interfaces.

```
config switch-controller auto-config default
    Description: Policies which are applied automatically to all ISL/ICL/FortiLink interfaces.
    set fgt-policy {string}
    set icl-policy {string}
    set isl-policy {string}
end
```

config switch-controller auto-config default

Parameter	Description	Type	Size	Default
fgt-policy	Default FortiLink auto-config policy.	string	Maximum length: 63	default
icl-policy	Default ICL auto-config policy.	string	Maximum length: 63	default-icl
isl-policy	Default ISL auto-config policy.	string	Maximum length: 63	default

config switch-controller auto-config policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Policy definitions which can define the behavior on auto configured interfaces.

```
config switch-controller auto-config policy
  Description: Policy definitions which can define the behavior on auto configured interfaces.
  edit <name>
    set igmp-flood-report [enable|disable]
    set igmp-flood-traffic [enable|disable]
    set poe-status [enable|disable]
    set qos-policy {string}
    set storm-control-policy {string}
  next
end
```

config switch-controller auto-config policy

Parameter	Description	Type	Size	Default
igmp-flood-report	Enable/disable IGMP flood report.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable IGMP flood report.		
	<i>disable</i>	Disable IGMP flood report.		
igmp-flood-traffic	Enable/disable IGMP flood traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IGMP flood traffic.		
	<i>disable</i>	Disable IGMP flood traffic.		
name	Auto-config policy name.	string	Maximum length: 63	
poe-status	Enable/disable PoE status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable PoE status.		
	<i>disable</i>	Disable PoE status.		
qos-policy	Auto-Config QoS policy.	string	Maximum length: 63	default
storm-control-policy	Auto-Config storm control policy.	string	Maximum length: 63	auto-config

config switch-controller custom-command



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure the FortiGate switch controller to send custom commands to managed FortiSwitch devices.

```
config switch-controller custom-command
    Description: Configure the FortiGate switch controller to send custom commands to managed
    FortiSwitch devices.
    edit <command-name>
        set command {var-string}
        set description {string}
    next
end
```

config switch-controller custom-command

Parameter	Description	Type	Size	Default
command	String of commands to send to FortiSwitch devices (For example (%0a = return key): config switch trunk %0a edit myTrunk %0a set members port1 port2 %0a end %0a).	var-string	Maximum length: 4095	
command-name	Command name called by the FortiGate switch controller in the execute command.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 35	

config switch-controller dsl policy



This command is available for model(s): FortiGate 40F 3G4G, FortiGate 60F, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F DSL, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R.

DSL policy.

```
config switch-controller dsl policy
  Description: DSL policy.
  edit <name>
    set append_padding [disable|enable]
    set cpe-aele [disable|enable]
    set cpe-aele-mode [ELE_M0|ELE_DS|...]
    set cs {option1}, {option2}, ...
    set ds-bitswap [disable|enable]
    set pause-frame [disable|enable]
    set profile [auto-30a|auto-17a|...]
    set type {option}
    set us-bitswap [disable|enable]
  next
end
```

config switch-controller dsl policy

Parameter	Description	Type	Size	Default										
append_padding	Device pause frame configuration.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>enable</i></td><td>Enable.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.							
Option	Description													
<i>disable</i>	Disable.													
<i>enable</i>	Enable.													
cpe-aele	CPE AELE.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>enable</i></td><td>Enable.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.							
Option	Description													
<i>disable</i>	Disable.													
<i>enable</i>	Enable.													
cpe-aele-mode	CPE AELE-Mode with given string.	option	-	ELE_MIN										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ELE_M0</i></td><td>cpe AELE-Mode with given string.</td></tr><tr><td><i>ELE_DS</i></td><td>cpe AELE-Mode with given string.</td></tr><tr><td><i>ELE_PB</i></td><td>cpe AELE-Mode with given string.</td></tr><tr><td><i>ELE_MIN</i></td><td>cpe AELE-Mode with given string.</td></tr></table>	Option	Description	<i>ELE_M0</i>	cpe AELE-Mode with given string.	<i>ELE_DS</i>	cpe AELE-Mode with given string.	<i>ELE_PB</i>	cpe AELE-Mode with given string.	<i>ELE_MIN</i>	cpe AELE-Mode with given string.			
Option	Description													
<i>ELE_M0</i>	cpe AELE-Mode with given string.													
<i>ELE_DS</i>	cpe AELE-Mode with given string.													
<i>ELE_PB</i>	cpe AELE-Mode with given string.													
<i>ELE_MIN</i>	cpe AELE-Mode with given string.													
cs	CPE carrier set.	option	-	A43 B43 A43C										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>A43</i></td><td>CPE carrier set.</td></tr><tr><td><i>B43</i></td><td>CPE carrier set.</td></tr><tr><td><i>A43C</i></td><td>CPE carrier set.</td></tr><tr><td><i>V43</i></td><td>CPE carrier set.</td></tr></table>	Option	Description	<i>A43</i>	CPE carrier set.	<i>B43</i>	CPE carrier set.	<i>A43C</i>	CPE carrier set.	<i>V43</i>	CPE carrier set.			
Option	Description													
<i>A43</i>	CPE carrier set.													
<i>B43</i>	CPE carrier set.													
<i>A43C</i>	CPE carrier set.													
<i>V43</i>	CPE carrier set.													
ds-bitswap	Enable/disable bitswap.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>enable</i></td><td>Enable.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.							
Option	Description													
<i>disable</i>	Disable.													
<i>enable</i>	Enable.													

Parameter	Description	Type	Size	Default
name	Policy name.	string	Maximum length: 63	
pause-frame	Device pause frame configuration.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		
profile	VDSL CPE profile.	option	-	auto-30a
	Option	Description		
	<i>auto-30a</i>	vdsl CPE profile.		
	<i>auto-17a</i>	vdsl CPE profile.		
	<i>auto-12ab</i>	vdsl CPE profile.		
type	Type.	option	-	Proscend
	Option	Description		
	<i>Proscend</i>	Proscend.		
us-bitswap	Enable/disable bitswap.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		

config switch-controller dynamic-port-policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure Dynamic port policy to be applied on the managed FortiSwitch ports through DPP device.

```
config switch-controller dynamic-port-policy
  Description: Configure Dynamic port policy to be applied on the managed FortiSwitch ports
  through DPP device.
  edit <name>
    set description {string}
    set fortilink {string}
    config policy
      Description: Port policies with matching criteria and actions.
      edit <name>
        set 802-1x {string}
        set bounce-port-duration {integer}
        set bounce-port-link [disable|enable]
        set category [device|interface-tag]
        set description {string}
        set family {string}
        set host {string}
        set hw-vendor {string}
        set interface-tags <tag-name1>, <tag-name2>, ...
        set lldp-profile {string}
        set mac {string}
        set match-period {integer}
        set match-remove [default|link-down]
```

```

        set match-type [dynamic|override]
        set poe-reset [disable|enable]
        set qos-policy {string}
        set status [enable|disable]
        set type {string}
        set vlan-policy {string}
    next
end
next
end

```

config switch-controller dynamic-port-policy

Parameter	Description	Type	Size	Default
description	Description for the Dynamic port policy.	string	Maximum length: 63	
fortilink	FortiLink interface for which this Dynamic port policy belongs to.	string	Maximum length: 15	
name	Dynamic port policy name.	string	Maximum length: 63	

config policy

Parameter	Description	Type	Size	Default						
802-1x	802.1x security policy to be applied when using this policy.	string	Maximum length: 31							
bounce-port-duration	Bounce duration in seconds of a switch port where this policy is applied.	integer	Minimum value: 1 Maximum value: 30	5						
bounce-port-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where this policy is applied. Helps to clear and reassign VLAN from lldp-profile.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.</td></tr><tr><td><i>enable</i></td><td>Enable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.</td></tr></table>				Option	Description	<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.	<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.
Option	Description									
<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.									
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.									
category	Category of Dynamic port policy.	option	-	device						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>device</i></td><td>Device category.</td></tr><tr><td><i>interface-tag</i></td><td>Interface Tag category.</td></tr></table>	Option	Description	<i>device</i>	Device category.	<i>interface-tag</i>	Interface Tag category.			
	Option	Description								
	<i>device</i>	Device category.								
<i>interface-tag</i>	Interface Tag category.									
description	Description for the policy.	string	Maximum length: 63							
family	Match policy based on family.	string	Maximum length: 31							
host	Match policy based on host.	string	Maximum length: 64							
hw-vendor	Match policy based on hardware vendor.	string	Maximum length: 15							
interface-tags <tag-name>	Match policy based on the FortiSwitch interface object tags. FortiSwitch port tag name.	string	Maximum length: 63							
lldp-profile	LLDP profile to be applied when using this policy.	string	Maximum length: 63							
mac	Match policy based on MAC address.	string	Maximum length: 17							
match-period	Number of days the matched devices will be retained (0 - 120, 0 = always retain).	integer	Minimum value: 0 Maximum value: 120	0						
match-remove	Options to remove the matched override devices.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Remove the matched override devices based on the match period.</td></tr><tr><td><i>link-down</i></td><td>Remove the matched override devices based on switch port link down event.</td></tr></table>	Option	Description	<i>default</i>	Remove the matched override devices based on the match period.	<i>link-down</i>	Remove the matched override devices based on switch port link down event.			
	Option	Description								
	<i>default</i>	Remove the matched override devices based on the match period.								
<i>link-down</i>	Remove the matched override devices based on switch port link down event.									
match-type	Match and retain the devices based on the type.	option	-	dynamic						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dynamic</i></td><td>Matched devices will be removed on dynamic events like link-down,device-inactivity,switch-offline.</td></tr><tr><td><i>override</i></td><td>Matched devices will be retained until the match-period.</td></tr></table>	Option	Description	<i>dynamic</i>	Matched devices will be removed on dynamic events like link-down,device-inactivity,switch-offline.	<i>override</i>	Matched devices will be retained until the match-period.			
	Option	Description								
	<i>dynamic</i>	Matched devices will be removed on dynamic events like link-down,device-inactivity,switch-offline.								
<i>override</i>	Matched devices will be retained until the match-period.									

Parameter	Description	Type	Size	Default
name	Policy name.	string	Maximum length: 63	
poe-reset	Enable/disable POE reset of a switch port where this policy is applied.	option	-	disable
	Option	Description		
	disable	Disable POE reset of a switch port where this policy is applied.		
	enable	Enable POE reset of a switch port where this policy is applied.		
qos-policy	QoS policy to be applied when using this policy.	string	Maximum length: 63	
status	Enable/disable policy.	option	-	enable
	Option	Description		
	enable	Enable policy.		
	disable	Disable policy.		
type	Match policy based on type.	string	Maximum length: 15	
vlan-policy	VLAN policy to be applied when using this policy.	string	Maximum length: 63	

config switch-controller flow-tracking



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch flow tracking and export via ipfix/netflow.

```
config switch-controller flow-tracking
  Description: Configure FortiSwitch flow tracking and export via ipfix/netflow.
  config aggregates
    Description: Configure aggregates in which all traffic sessions matching the IP Address
    will be grouped into the same flow.
    edit <id>
      set ip {ipv4-classnet}
    next
  end
  config collectors
    Description: Configure collectors for the flow.
    edit <name>
      set ip {ipv4-address-any}
      set port {integer}
      set transport [udp|tcp|...]
    next
  end
  set format [netflow1|netflow5|...]
  set level [vlan|ip|...]
  set max-export-pkt-size {integer}
  set sample-mode [local|perimeter|...]
  set sample-rate {integer}
```



```

set template-export-period {integer}
set timeout-general {integer}
set timeout-icmp {integer}
set timeout-max {integer}
set timeout-tcp {integer}
set timeout-tcp-fin {integer}
set timeout-tcp-rst {integer}
set timeout-udp {integer}
end

```

config switch-controller flow-tracking

Parameter	Description	Type	Size	Default												
format	Configure flow tracking protocol.	option	-	netflow9												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>netflow1</td><td>Netflow version 1 sampling.</td></tr><tr><td>netflow5</td><td>Netflow version 5 sampling.</td></tr><tr><td>netflow9</td><td>Netflow version 9 sampling.</td></tr><tr><td>ipfix</td><td>Ipfix sampling.</td></tr></table>	Option	Description	netflow1	Netflow version 1 sampling.	netflow5	Netflow version 5 sampling.	netflow9	Netflow version 9 sampling.	ipfix	Ipfix sampling.					
Option	Description															
netflow1	Netflow version 1 sampling.															
netflow5	Netflow version 5 sampling.															
netflow9	Netflow version 9 sampling.															
ipfix	Ipfix sampling.															
level	Configure flow tracking level.	option	-	ip												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>vlan</td><td>Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.</td></tr><tr><td>ip</td><td>Collects srcip/dstip from the sample packet.</td></tr><tr><td>port</td><td>Collects srcip/dstip/srcport/dstport/protocol from the sample packet.</td></tr><tr><td>proto</td><td>Collects srcip/dstip/protocol from the sample packet.</td></tr><tr><td>mac</td><td>Collects smac/dmac from the sample packet.</td></tr></table>	Option	Description	vlan	Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.	ip	Collects srcip/dstip from the sample packet.	port	Collects srcip/dstip/srcport/dstport/protocol from the sample packet.	proto	Collects srcip/dstip/protocol from the sample packet.	mac	Collects smac/dmac from the sample packet.			
Option	Description															
vlan	Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.															
ip	Collects srcip/dstip from the sample packet.															
port	Collects srcip/dstip/srcport/dstport/protocol from the sample packet.															
proto	Collects srcip/dstip/protocol from the sample packet.															
mac	Collects smac/dmac from the sample packet.															
max-export-pkt-size	Configure flow max export packet size (512-9216, default=512 bytes).	integer	Minimum value: 512 Maximum value: 9216	512												
sample-mode	Configure sample mode for the flow tracking.	option	-	perimeter												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>local</td><td>Set local mode which samples on the specific switch port.</td></tr></table>	Option	Description	local	Set local mode which samples on the specific switch port.											
Option	Description															
local	Set local mode which samples on the specific switch port.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>perimeter</i>	Set perimeter mode which samples on all switch fabric ports and fortilink port at the ingress.		
	<i>device-ingress</i>	Set device -ingress mode which samples across all switch ports at the ingress.		
sample-rate	Configure sample rate for the perimeter and device-ingress sampling(0 - 99999).	integer	Minimum value: 0 Maximum value: 99999	512
template-export-period	Configure template export period (1-60, default=5 minutes).	integer	Minimum value: 1 Maximum value: 60	5
timeout-general	Configure flow session general timeout (60-604800, default=3600 seconds).	integer	Minimum value: 60 Maximum value: 604800	3600
timeout-icmp	Configure flow session ICMP timeout (60-604800, default=300 seconds).	integer	Minimum value: 60 Maximum value: 604800	300
timeout-max	Configure flow session max timeout (60-604800, default=604800 seconds).	integer	Minimum value: 60 Maximum value: 604800	604800
timeout-tcp	Configure flow session TCP timeout (60-604800, default=3600 seconds).	integer	Minimum value: 60 Maximum value: 604800	3600
timeout-tcp-fin	Configure flow session TCP FIN timeout (60-604800, default=300 seconds).	integer	Minimum value: 60 Maximum value: 604800	300
timeout-tcp-rst	Configure flow session TCP RST timeout (60-604800, default=120 seconds).	integer	Minimum value: 60 Maximum value: 604800	120
timeout-udp	Configure flow session UDP timeout (60-604800, default=300 seconds).	integer	Minimum value: 60 Maximum value: 604800	300

config aggregates

Parameter	Description	Type	Size	Default
id	Aggregate id.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
ip	IP address to group all matching traffic sessions to a flow.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config collectors

Parameter	Description	Type	Size	Default
ip	Collector IP address.	ipv4-address-any	Not Specified	0.0.0.0
name	Collector name.	string	Maximum length: 63	
port	Collector port number(0-65535, default:0, netflow:2055, ipfix:4739).	integer	Minimum value: 0 Maximum value: 65535	0
transport	Collector L4 transport protocol for exporting packets.	option	-	udp
		Option	Description	
		udp	UDP protocol.	
		tcp	TCP protocol.	
		sctp	SCTP protocol.	

config switch-controller fortilink-settings



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure integrated FortiLink settings for FortiSwitch.

```
config switch-controller fortilink-settings
  Description: Configure integrated FortiLink settings for FortiSwitch.
  edit <name>
    set access-vlan-mode [legacy|fail-open|...]
    set fortilink {string}
    set inactive-timer {integer}
    set link-down-flush [disable|enable]
    config nac-ports
      Description: NAC specific configuration.
      set lan-segment [enabled|disabled]
      set member-change {integer}
      set nac-lan-interface {string}
      set nac-segment-vlans <vlan-name1>, <vlan-name2>, ...
      set onboarding-vlan {string}
      set parent-key {string}
    end
  next
end
```

config switch-controller fortilink-settings

Parameter	Description	Type	Size	Default
access-vlan-mode	Intra VLAN traffic behavior with loss of connection to the FortiGate.	option	-	legacy
	Option	Description		
	legacy	Backward compatible behavior.		
	fail-open	When connection to FortiGate is lost, traffic on the VLAN may continue directly between end points.		
	fail-close	When connection to FortiGate is lost, traffic between endpoints on the VLAN is blocked.		
fortilink	FortiLink interface to which this fortilink-setting belongs.	string	Maximum length: 15	
inactive-timer	Time interval(minutes) to be included in the inactive devices expiry calculation (mac age-out + inactive-time + periodic scan interval).	integer	Minimum value: 1 Maximum value: 1440	15
link-down-flush	Clear NAC and dynamic devices on switch ports on link down event.	option	-	enable
	Option	Description		
	disable	Disable clearing NAC and dynamic devices on a switch port when link down event happens.		
	enable	Enable clearing NAC and dynamic devices on a switch port when link down event happens.		
name	FortiLink settings name.	string	Maximum length: 35	

config nac-ports

Parameter	Description	Type	Size	Default						
lan-segment	Enable/disable LAN segment feature on the FortiLink interface.	option	-	disabled						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enabled</i></td><td>Enable lan-segment on this interface.</td></tr><tr><td><i>disabled</i></td><td>Disable lan-segment on this interface.</td></tr></table>				Option	Description	<i>enabled</i>	Enable lan-segment on this interface.	<i>disabled</i>	Disable lan-segment on this interface.
Option	Description									
<i>enabled</i>	Enable lan-segment on this interface.									
<i>disabled</i>	Disable lan-segment on this interface.									

Parameter	Description	Type	Size	Default
member-change	Member change flag. Read-only.	integer	Minimum value: 0 Maximum value: 255	0
nac-lan-interface	Configure NAC LAN interface.	string	Maximum length: 15	
nac-segment-vlans <vlan-name>	Configure NAC segment VLANs. VLAN interface name.	string	Maximum length: 79	
onboarding-vlan	Default NAC Onboarding VLAN when NAC devices are discovered.	string	Maximum length: 15	
parent-key	Parent key name. Read-only.	string	Maximum length: 35	

config switch-controller global



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R. It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch global settings.

```
config switch-controller global
    Description: Configure FortiSwitch global settings.
```

```

set bounce-quarantined-link [disable|enable]
config custom-command
    Description: List of custom commands to be pushed to all FortiSwitches in the VDOM.
    edit <command-entry>
        set command-name {string}
    next
end
set default-virtual-switch-vlan {string}
set dhcp-option82-circuit-id {option1}, {option2}, ...
set dhcp-option82-format [ascii|legacy]
set dhcp-option82-remote-id {option1}, {option2}, ...
set dhcp-server-access-list [enable|disable]
set dhcp-snoop-client-db-exp {integer}
set dhcp-snoop-client-req [drop-untrusted|forward-untrusted]
set dhcp-snoop-db-per-port-learn-limit {integer}
set disable-discovery <name1>, <name2>, ...
set fips-enforce [disable|enable]
set firmware-provision-on-authorization [enable|disable]
set https-image-push [enable|disable]
set log-mac-limit-violations [enable|disable]
set mac-aging-interval {integer}
set mac-event-logging [enable|disable]
set mac-retention-period {integer}
set mac-violation-timer {integer}
set quarantine-mode [by-vlan|by-redirect]
set sn-dns-resolution [enable|disable]
set switch-on-deauth [no-op|factory-reset]
set update-user-device {option1}, {option2}, ...
set vlan-all-mode [all|defined]
set vlan-identity [description|name]
set vlan-optimization [prune|configured|...]
end

```

config switch-controller global

Parameter	Description	Type	Size	Default
bounce-quarantined-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last. Helps to re-initiate the DHCP process for a device.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td></tr></table>	Option	Description	<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.											
	Option	Description														
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.															
default-virtual-switch-vlan	Default VLAN for ports when added to the virtual-switch.	string	Maximum length: 15													
dhcp-option82-circuit-id	List the parameters to be included to inform about client identification.	option	-	intfname vlan mode												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>intfname</i></td><td>Interface name.</td></tr><tr><td><i>vlan</i></td><td>VLAN name.</td></tr><tr><td><i>hostname</i></td><td>Hostname.</td></tr><tr><td><i>mode</i></td><td>Mode.</td></tr><tr><td><i>description</i></td><td>Description.</td></tr></table>	Option	Description	<i>intfname</i>	Interface name.	<i>vlan</i>	VLAN name.	<i>hostname</i>	Hostname.	<i>mode</i>	Mode.	<i>description</i>	Description.			
	Option	Description														
	<i>intfname</i>	Interface name.														
	<i>vlan</i>	VLAN name.														
	<i>hostname</i>	Hostname.														
	<i>mode</i>	Mode.														
<i>description</i>	Description.															
dhcp-option82-format	DHCP option-82 format string.	option	-	ascii												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ascii</i></td><td>Allow user to choose values for circuit-id and remote-id. Format: cid=[hostname,interface,mode,vlan,description] rid=[hostname,xx:xx:xx:xx:xx:xx,ip]</td></tr><tr><td><i>legacy</i></td><td>Generate predefined fixed format for circuit-id and remote. Format: cid=hostname-[<vlan:16><mod:8><port:8>].32bit, rid= [mac (0.6)].48bit</td></tr></table>	Option	Description	<i>ascii</i>	Allow user to choose values for circuit-id and remote-id. Format: cid=[hostname,interface,mode,vlan,description] rid=[hostname,xx:xx:xx:xx:xx:xx,ip]	<i>legacy</i>	Generate predefined fixed format for circuit-id and remote. Format: cid=hostname-[<vlan:16><mod:8><port:8>].32bit, rid= [mac (0.6)].48bit									
	Option	Description														
	<i>ascii</i>	Allow user to choose values for circuit-id and remote-id. Format: cid=[hostname,interface,mode,vlan,description] rid=[hostname,xx:xx:xx:xx:xx:xx,ip]														
<i>legacy</i>	Generate predefined fixed format for circuit-id and remote. Format: cid=hostname-[<vlan:16><mod:8><port:8>].32bit, rid= [mac (0.6)].48bit															
dhcp-option82-remote-id	List the parameters to be included to inform about client identification.	option	-	mac												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mac</i></td><td>MAC address.</td></tr><tr><td><i>hostname</i></td><td>Hostname.</td></tr><tr><td><i>ip</i></td><td>IP address.</td></tr></table>	Option	Description	<i>mac</i>	MAC address.	<i>hostname</i>	Hostname.	<i>ip</i>	IP address.							
	Option	Description														
	<i>mac</i>	MAC address.														
	<i>hostname</i>	Hostname.														
<i>ip</i>	IP address.															
dhcp-server-access-list	Enable/disable DHCP snooping server access list.	option	-	disable												

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable DHCP server access list.		
	<i>disable</i>	Disable DHCP server access list.		
dhcp-snoop-client-db-exp	Expiry time for DHCP snooping server database entries (300 - 259200 sec, default = 86400 sec).	integer	Minimum value: 300 Maximum value: 259200	86400
dhcp-snoop-client-req	Client DHCP packet broadcast mode.	option	-	drop-untrusted
	Option Description			
	<i>drop-untrusted</i>	Broadcast packets on trusted ports in the VLAN.		
	<i>forward-untrusted</i>	Broadcast packets on all ports in the VLAN.		
dhcp-snoop-db-per-port-learn-limit	Per Interface dhcp-server entries learn limit (0 - 1024, default = 64).	integer	Minimum value: 0 Maximum value: 2048	64
disable-discovery <name>	Prevent this FortiSwitch from discovering Managed device ID.	string	Maximum length: 79	
fips-enforce	Enable/disable enforcement of FIPS on managed FortiSwitch devices.	option	-	enable
	Option Description			
	<i>disable</i>	Disable enforcement of FIPS on managed FortiSwitch devices.		
	<i>enable</i>	Enable enforcement of FIPS on managed FortiSwitch devices.		
firmware-provision-on-authorization	Enable/disable automatic provisioning of latest firmware on authorization.	option	-	disable
	Option Description			
	<i>enable</i>	Enable firmware provision on authorization.		
	<i>disable</i>	Disable firmware provision on authorization.		
https-image-push	Enable/disable image push to FortiSwitch using HTTPS.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable image push to FortiSwitch using HTTPS.		
	<i>disable</i>	Disable image push to FortiSwitch using HTTPS.		
log-mac-limit-violations	Enable/disable logs for Learning Limit Violations.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Learn Limit Violation.		
	<i>disable</i>	Disable Learn Limit Violation.		
mac-aging-interval	Time after which an inactive MAC is aged out (10 - 1000000 sec, default = 300, 0 = disable).	integer	Minimum value: 10 Maximum value: 1000000	300
mac-event-logging	Enable/disable MAC address event logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable MAC address event logging.		
	<i>disable</i>	Disable MAC address event logging.		
mac-retention-period	Time in hours after which an inactive MAC is removed from client DB (0 = aged out based on mac-aging-interval).	integer	Minimum value: 0 Maximum value: 168	24
mac-violation-timer	Set timeout for Learning Limit Violations (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
quarantine-mode	Quarantine mode.	option	-	by-vlan
	Option	Description		
	<i>by-vlan</i>	Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.		
	<i>by-redirect</i>	Quarantined device traffic is redirected only to the FortiGate on the received VLAN.		
sn-dns-resolution	Enable/disable DNS resolution of the FortiSwitch unit's IP address with switch name.	option	-	enable

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DNS resolution of the FortiSwitch unit's IP address with switch name.</td></tr><tr><td><i>disable</i></td><td>Disable DNS resolution of the FortiSwitch unit's IP address with switch name.</td></tr></table>	Option	Description	<i>enable</i>	Enable DNS resolution of the FortiSwitch unit's IP address with switch name.	<i>disable</i>	Disable DNS resolution of the FortiSwitch unit's IP address with switch name.									
	Option	Description														
	<i>enable</i>	Enable DNS resolution of the FortiSwitch unit's IP address with switch name.														
<i>disable</i>	Disable DNS resolution of the FortiSwitch unit's IP address with switch name.															
switch-on-deauth	No-operation/Factory-reset the managed FortiSwitch on deauthorization.	option	-	no-op												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-op</i></td><td>No-operation on the managed FortiSwitch on deauthorization.</td></tr><tr><td><i>factory-reset</i></td><td>Factory-reset the managed FortiSwitch on deauthorization.</td></tr></table>	Option	Description	<i>no-op</i>	No-operation on the managed FortiSwitch on deauthorization.	<i>factory-reset</i>	Factory-reset the managed FortiSwitch on deauthorization.									
	Option	Description														
	<i>no-op</i>	No-operation on the managed FortiSwitch on deauthorization.														
<i>factory-reset</i>	Factory-reset the managed FortiSwitch on deauthorization.															
update-user-device	Control which sources update the device user list.	option	-	mac-cache lldp dhcp-snooping l2-db l3-db												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mac-cache</i></td><td>Update MAC address from switch-controller mac-cache.</td></tr><tr><td><i>lldp</i></td><td>Update from FortiSwitch LLDP neighbor database.</td></tr><tr><td><i>dhcp-snooping</i></td><td>Update from FortiSwitch DHCP snooping client and server databases.</td></tr><tr><td><i>l2-db</i></td><td>Update from FortiSwitch Network-monitor Layer 2 tracking database.</td></tr><tr><td><i>l3-db</i></td><td>Update from FortiSwitch Network-monitor Layer 3 tracking database.</td></tr></table>	Option	Description	<i>mac-cache</i>	Update MAC address from switch-controller mac-cache.	<i>lldp</i>	Update from FortiSwitch LLDP neighbor database.	<i>dhcp-snooping</i>	Update from FortiSwitch DHCP snooping client and server databases.	<i>l2-db</i>	Update from FortiSwitch Network-monitor Layer 2 tracking database.	<i>l3-db</i>	Update from FortiSwitch Network-monitor Layer 3 tracking database.			
	Option	Description														
	<i>mac-cache</i>	Update MAC address from switch-controller mac-cache.														
	<i>lldp</i>	Update from FortiSwitch LLDP neighbor database.														
	<i>dhcp-snooping</i>	Update from FortiSwitch DHCP snooping client and server databases.														
	<i>l2-db</i>	Update from FortiSwitch Network-monitor Layer 2 tracking database.														
<i>l3-db</i>	Update from FortiSwitch Network-monitor Layer 3 tracking database.															
vlan-all-mode	VLAN configuration mode, user-defined-vlans or all-possible-vlans.	option	-	defined												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Include all possible VLANs (1-4093).</td></tr><tr><td><i>defined</i></td><td>Include user defined VLANs.</td></tr></table>	Option	Description	<i>all</i>	Include all possible VLANs (1-4093).	<i>defined</i>	Include user defined VLANs.									
	Option	Description														
	<i>all</i>	Include all possible VLANs (1-4093).														
<i>defined</i>	Include user defined VLANs.															
vlan-identity	Identity of the VLAN. Commonly used for RADIUS Tunnel-Private-Group-Id.	option	-	name												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>description</i></td><td>Configure the VLAN description to that of the FortiOS interface description if available; otherwise use the interface name.</td></tr><tr><td><i>name</i></td><td>Configure the VLAN description to that of the FortiOS interface name.</td></tr></table>	Option	Description	<i>description</i>	Configure the VLAN description to that of the FortiOS interface description if available; otherwise use the interface name.	<i>name</i>	Configure the VLAN description to that of the FortiOS interface name.									
	Option	Description														
	<i>description</i>	Configure the VLAN description to that of the FortiOS interface description if available; otherwise use the interface name.														
<i>name</i>	Configure the VLAN description to that of the FortiOS interface name.															

Parameter	Description	Type	Size	Default
vlan-optimization	FortiLink VLAN optimization.	option	-	configured
	Option	Description		
	<i>prune</i>	Enable VLAN optimization (only VLANs necessary on or along path between destinations) on FortiSwitch units for auto-generated trunks.		
	<i>configured</i>	Enable VLAN optimization (only VLANs created on Fortilink interface) on FortiSwitch units for auto-generated trunks.		
	<i>none</i>	Disable VLAN optimization on FortiSwitch units for auto-generated trunks.		

config custom-command

Parameter	Description	Type	Size	Default
command-entry	List of FortiSwitch commands.	string	Maximum length: 35	
command-name	Name of custom command to push to all FortiSwitches in VDOM.	string	Maximum length: 35	

config switch-controller igmp-snooping



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch IGMP snooping global settings.

```
config switch-controller igmp-snooping
  Description: Configure FortiSwitch IGMP snooping global settings.
  set aging-time {integer}
  set flood-unknown-multicast [enable|disable]
  set query-interval {integer}
end
```

config switch-controller igmp-snooping

Parameter	Description	Type	Size	Default						
aging-time	Maximum number of seconds to retain a multicast snooping entry for which no packets have been seen (15 - 3600 sec, default = 300).	integer	Minimum value: 15 Maximum value: 3600	300						
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable unknown multicast flooding.</td></tr><tr><td>disable</td><td>Disable unknown multicast flooding.</td></tr></table>				Option	Description	enable	Enable unknown multicast flooding.	disable	Disable unknown multicast flooding.
Option	Description									
enable	Enable unknown multicast flooding.									
disable	Disable unknown multicast flooding.									
query-interval	Maximum time after which IGMP query will be sent (10 - 1200 sec, default = 125).	integer	Minimum value: 10 Maximum value: 1200	125						

config switch-controller initial-config template



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure template for auto-generated VLANs.

```
config switch-controller initial-config template
  Description: Configure template for auto-generated VLANs.
  edit <name>
    set allowaccess {option1}, {option2}, ...
    set auto-ip [enable|disable]
    set dhcp-server [enable|disable]
    set ip {ipv4-classnet-host}
    set vlanid {integer}
  next
end
```

config switch-controller initial-config template

Parameter	Description	Type	Size	Default
allowaccess	Permitted types of management access to this interface.	option	-	

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>fgfm</i></td><td>FortiManager access.</td></tr><tr><td><i>radius-acct</i></td><td>RADIUS accounting access.</td></tr><tr><td><i>probe-response</i></td><td>Probe access.</td></tr><tr><td><i>fabric</i></td><td>Security Fabric access.</td></tr><tr><td><i>ftm</i></td><td>FTM access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.	<i>probe-response</i>	Probe access.	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.			
	Option	Description																										
	<i>ping</i>	PING access.																										
	<i>https</i>	HTTPS access.																										
	<i>ssh</i>	SSH access.																										
	<i>snmp</i>	SNMP access.																										
	<i>http</i>	HTTP access.																										
	<i>telnet</i>	TELNET access.																										
	<i>fgfm</i>	FortiManager access.																										
	<i>radius-acct</i>	RADIUS accounting access.																										
	<i>probe-response</i>	Probe access.																										
	<i>fabric</i>	Security Fabric access.																										
<i>ftm</i>	FTM access.																											
auto-ip	Automatically allocate interface address and subnet block.	option	-	enable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auto-ip status.</td></tr><tr><td><i>disable</i></td><td>Disable auto-ip status.</td></tr></table>	Option	Description	<i>enable</i>	Enable auto-ip status.	<i>disable</i>	Disable auto-ip status.																					
	Option	Description																										
	<i>enable</i>	Enable auto-ip status.																										
<i>disable</i>	Disable auto-ip status.																											
dhcp-server	Enable/disable a DHCP server on this interface.	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP server.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP server.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP server.	<i>disable</i>	Disable DHCP server.																					
	Option	Description																										
	<i>enable</i>	Enable DHCP server.																										
<i>disable</i>	Disable DHCP server.																											
ip	Interface IPv4 address and subnet mask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																								
name	Initial config template name.	string	Maximum length: 63																									
vlanid	Unique VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0																								

config switch-controller initial-config vlans



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure initial template for auto-generated VLAN interfaces.

```
config switch-controller initial-config vlans
  Description: Configure initial template for auto-generated VLAN interfaces.
  set default-vlan {string}
  set nac {string}
  set nac-segment {string}
  set optional-vlans [enable|disable]
  set quarantine {string}
  set rspan {string}
  set video {string}
  set voice {string}
end
```

config switch-controller initial-config vlans

Parameter	Description	Type	Size	Default
default-vlan	Default VLAN (native) assigned to all switch ports upon discovery.	string	Maximum length: 63	_default

Parameter	Description	Type	Size	Default						
nac	VLAN for NAC onboarding devices.	string	Maximum length: 63	onboarding						
nac-segment	VLAN for NAC segment primary interface.	string	Maximum length: 63	nac_segment						
optional-vlans	Auto-generate pre-configured VLANs upon switch discovery.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable auto-generated VLANs.</td></tr><tr><td>disable</td><td>Disable auto-generated VLANs.</td></tr></table>				Option	Description	enable	Enable auto-generated VLANs.	disable	Disable auto-generated VLANs.
	Option	Description								
	enable	Enable auto-generated VLANs.								
disable	Disable auto-generated VLANs.									
quarantine	VLAN for quarantined traffic.	string	Maximum length: 63	quarantine						
rspan	VLAN for RSPAN/ERSPAN mirrored traffic.	string	Maximum length: 63	rspan						
video	VLAN dedicated for video devices.	string	Maximum length: 63	video						
voice	VLAN dedicated for voice devices.	string	Maximum length: 63	voice						

config switch-controller lldp-profile



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch LLDP profiles.

```
config switch-controller lldp-profile
  Description: Configure FortiSwitch LLDP profiles.
  edit <name>
    set 802 1-tlvs {option1}, {option2}, ...
    set 802 3-tlvs {option1}, {option2}, ...
    set auto-is1 [disable|enable]
    set auto-is1-auth [legacy|strict|...]
    set auto-is1-auth-encrypt [none|mixed|...]
    set auto-is1-auth-identity {string}
    set auto-is1-auth-macsec-profile {string}
    set auto-is1-auth-reauth {integer}
    set auto-is1-auth-user {string}
    set auto-is1-hello-timer {integer}
    set auto-is1-port-group {integer}
    set auto-is1-receive-timeout {integer}
    set auto-mclag-icl [disable|enable]
  config custom-tlvs
    Description: Configuration method to edit custom TLV entries.
    edit <name>
      set information-string {user}
      set oui {user}
      set subtype {integer}
```

```

    next
end
config med-location-service
    Description: Configuration method to edit Media Endpoint Discovery (MED) location
service type-length-value (TLV) categories.
    edit <name>
        set status [disable|enable]
        set sys-location-id {string}
    next
end
config med-network-policy
    Description: Configuration method to edit Media Endpoint Discovery (MED) network
policy type-length-value (TLV) categories.
    edit <name>
        set assign-vlan [disable|enable]
        set dscp {integer}
        set priority {integer}
        set status [disable|enable]
        set vlan-intf {string}
    next
end
set med-tlvs {option1}, {option2}, ...
next
end

```

config switch-controller lldp-profile

Parameter	Description	Type	Size	Default						
802 1-tlvs	Transmitted IEEE 802.1 TLVs.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>port-vlan-id</i></td><td>Port native VLAN TLV.</td></tr></table>	Option	Description	<i>port-vlan-id</i>	Port native VLAN TLV.					
Option	Description									
<i>port-vlan-id</i>	Port native VLAN TLV.									
802 3-tlvs	Transmitted IEEE 802.3 TLVs.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>max-frame-size</i></td><td>Maximum frame size TLV.</td></tr><tr><td><i>power-negotiation</i></td><td>PoE+ classification TLV.</td></tr></table>	Option	Description	<i>max-frame-size</i>	Maximum frame size TLV.	<i>power-negotiation</i>	PoE+ classification TLV.			
Option	Description									
<i>max-frame-size</i>	Maximum frame size TLV.									
<i>power-negotiation</i>	PoE+ classification TLV.									
auto-isl	Enable/disable auto inter-switch LAG.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable automatic MCLAG inter chassis link.</td></tr><tr><td><i>enable</i></td><td>Enable automatic MCLAG inter chassis link.</td></tr></table>	Option	Description	<i>disable</i>	Disable automatic MCLAG inter chassis link.	<i>enable</i>	Enable automatic MCLAG inter chassis link.			
Option	Description									
<i>disable</i>	Disable automatic MCLAG inter chassis link.									
<i>enable</i>	Enable automatic MCLAG inter chassis link.									

Parameter	Description	Type	Size	Default								
auto-isl-auth	Auto inter-switch LAG authentication mode.	option	-	legacy								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>legacy</td><td>No auto inter-switch-LAG authentication.</td></tr><tr><td>strict</td><td>Strict auto inter-switch-LAG authentication.</td></tr><tr><td>relax</td><td>Relax auto inter-switch-LAG authentication.</td></tr></table>	Option	Description	legacy	No auto inter-switch-LAG authentication.	strict	Strict auto inter-switch-LAG authentication.	relax	Relax auto inter-switch-LAG authentication.			
Option	Description											
legacy	No auto inter-switch-LAG authentication.											
strict	Strict auto inter-switch-LAG authentication.											
relax	Relax auto inter-switch-LAG authentication.											
auto-isl-auth-encrypt	Auto inter-switch LAG encryption mode.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No auto inter-switch-LAG encryption.</td></tr><tr><td>mixed</td><td>Mixed auto inter-switch-LAG encryption.</td></tr><tr><td>must</td><td>Must auto inter-switch-LAG encryption.</td></tr></table>	Option	Description	none	No auto inter-switch-LAG encryption.	mixed	Mixed auto inter-switch-LAG encryption.	must	Must auto inter-switch-LAG encryption.			
Option	Description											
none	No auto inter-switch-LAG encryption.											
mixed	Mixed auto inter-switch-LAG encryption.											
must	Must auto inter-switch-LAG encryption.											
auto-isl-auth-identity	Auto inter-switch LAG authentication identity.	string	Maximum length: 63									
auto-isl-auth-macsec-profile	Auto inter-switch LAG macsec profile for encryption.	string	Maximum length: 63									
auto-isl-auth-reauth	Auto inter-switch LAG authentication reauth period in seconds(10 - 3600, default = 3600).	integer	Minimum value: 180 Maximum value: 3600	3600								
auto-isl-auth-user	Auto inter-switch LAG authentication user certificate.	string	Maximum length: 63									
auto-isl-hello-timer	Auto inter-switch LAG hello timer duration (1 - 30 sec, default = 3).	integer	Minimum value: 1 Maximum value: 30	3								
auto-isl-port-group	Auto inter-switch LAG port group ID (0 - 9).	integer	Minimum value: 0 Maximum value: 9	0								
auto-isl-receive-timeout	Auto inter-switch LAG timeout if no response is received (3 - 90 sec, default = 9).	integer	Minimum value: 0 Maximum value: 90	60								

Parameter	Description	Type	Size	Default
auto-mclag-icl	Enable/disable MCLAG inter chassis link.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable auto inter-switch-LAG.		
	<i>enable</i>	Enable auto inter-switch-LAG.		
med-tlvs	Transmitted LLDP-MED TLVs (type-length-value descriptions).	option	-	
	Option	Description		
	<i>inventory-management</i>	Inventory management TLVs.		
	<i>network-policy</i>	Network policy TLVs.		
	<i>power-management</i>	Power manangement TLVs.		
	<i>location-identification</i>	Location identificaion TLVs.		
name	Profile name.	string	Maximum length: 63	

config custom-tlvs

Parameter	Description	Type	Size	Default
information-string	Organizationally defined information string (0 - 507 hexadecimal bytes).	user	Not Specified	
name	TLV name (not sent).	string	Maximum length: 63	
oui	Organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.	user	Not Specified	000000
subtype	Organizationally defined subtype (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0

config med-location-service

Parameter	Description	Type	Size	Default
name	Location service type name.	string	Maximum length: 63	
status	Enable or disable this TLV.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not transmit this location service TLV.		
	<i>enable</i>	Transmit this location service TLV.		
sys-location-id	Location service ID.	string	Maximum length: 63	

config med-network-policy

Parameter	Description	Type	Size	Default
assign-vlan	Enable/disable VLAN assignment when this profile is applied on managed FortiSwitch port.	option	-	disable
	Option	Description		
	disable	Disable VLAN assignment when this profile is applied on port.		
	enable	Enable VLAN assignment when this profile is applied on port.		
dscp	Advertised Differentiated Services Code Point (DSCP) value, a packet header value indicating the level of service requested for traffic, such as high priority or best effort delivery.	integer	Minimum value: 0 Maximum value: 63	0
name	Policy type name.	string	Maximum length: 63	
priority	Advertised Layer 2 priority (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	0
status	Enable or disable this TLV.	option	-	disable
	Option	Description		
	disable	Do not transmit this network policy TLV.		
	enable	Transmit this TLV if a VLAN has been added to the port.		
vlan-intf	VLAN interface to advertise; if configured on port.	string	Maximum length: 15	

config switch-controller lldp-settings



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch LLDP settings.

```
config switch-controller lldp-settings
  Description: Configure FortiSwitch LLDP settings.
  set device-detection [disable|enable]
  set fast-start-interval {integer}
  set management-interface [internal|mgmt]
  set tx-hold {integer}
  set tx-interval {integer}
end
```

config switch-controller lldp-settings

Parameter	Description	Type	Size	Default						
device-detection	Enable/disable dynamic detection of LLDP neighbor devices for VLAN assignment.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dynamic detection of LLDP neighbor devices.</td></tr><tr><td><i>enable</i></td><td>Enable dynamic detection of LLDP neighbor devices.</td></tr></table>				Option	Description	<i>disable</i>	Disable dynamic detection of LLDP neighbor devices.	<i>enable</i>	Enable dynamic detection of LLDP neighbor devices.
Option	Description									
<i>disable</i>	Disable dynamic detection of LLDP neighbor devices.									
<i>enable</i>	Enable dynamic detection of LLDP neighbor devices.									

Parameter	Description	Type	Size	Default
fast-start-interval	Frequency of LLDP PDU transmission from FortiSwitch for the first 4 packets when the link is up (2 - 5 sec, default = 2, 0 = disable fast start).	integer	Minimum value: 0 Maximum value: 255	2
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.	option	-	internal
	Option	Description		
	internal	Use internal interface.		
	mgmt	Use management interface.		
tx-hold	Number of tx-intervals before local LLDP data expires (1 - 16, default = 4). Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 1 Maximum value: 16	4
tx-interval	Frequency of LLDP PDU transmission from FortiSwitch (5 - 4095 sec, default = 30). Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 5 Maximum value: 4095	30

config switch-controller location



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch location services.

```
config switch-controller location
  Description: Configure FortiSwitch location services.
  edit <name>
    config address-civic
      Description: Configure location civic address.
      set additional {string}
      set additional-code {string}
      set block {string}
      set branch-road {string}
      set building {string}
      set city {string}
      set city-division {string}
      set country {string}
      set country-subdivision {string}
      set county {string}
      set direction {string}
      set floor {string}
      set landmark {string}
      set language {string}
      set name {string}
      set number {string}
      set number-suffix {string}
      set parent-key {string}
      set place-type {string}
      set post-office-box {string}
      set postal-community {string}
      set primary-road {string}
      set road-section {string}
      set room {string}
      set script {string}
      set seat {string}
      set street {string}
      set street-name-post-mod {string}
      set street-name-pre-mod {string}
      set street-suffix {string}
      set sub-branch-road {string}
      set trailing-str-suffix {string}
      set unit {string}
      set zip {string}
    end
    config coordinates
      Description: Configure location GPS coordinates.
      set altitude {string}
      set altitude-unit [m|f]
      set datum [WGS84|NAD83|...]
      set latitude {string}
      set longitude {string}
      set parent-key {string}
    end
    config elin-number
      Description: Configure location ELIN number.
```

```

        set elin-num {string}
        set parent-key {string}
    end
next
end

```

config switch-controller location

Parameter	Description	Type	Size	Default
name	Unique location item name.	string	Maximum length: 63	

config address-civic

Parameter	Description	Type	Size	Default
additional	Location additional details.	string	Maximum length: 47	
additional-code	Location additional code details.	string	Maximum length: 47	
block	Location block details.	string	Maximum length: 47	
branch-road	Location branch road details.	string	Maximum length: 47	
building	Location building details.	string	Maximum length: 47	
city	Location city details.	string	Maximum length: 47	
city-division	Location city division details.	string	Maximum length: 47	
country	The two-letter ISO 3166 country code in capital ASCII letters eg. US, CA, DK, DE.	string	Maximum length: 47	
country-subdivision	National subdivisions (state, canton, region, province, or prefecture).	string	Maximum length: 47	
county	County, parish, gun (JP), or district (IN).	string	Maximum length: 47	
direction	Leading street direction.	string	Maximum length: 47	
floor	Floor.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
landmark	Landmark or vanity address.	string	Maximum length: 47	
language	Language.	string	Maximum length: 47	
name	Name (residence and office occupant).	string	Maximum length: 47	
number	House number.	string	Maximum length: 47	
number-suffix	House number suffix.	string	Maximum length: 47	
parent-key	Parent key name. Read-only.	string	Maximum length: 63	
place-type	Place type.	string	Maximum length: 47	
post-office-box	Post office box.	string	Maximum length: 47	
postal-community	Postal community name.	string	Maximum length: 47	
primary-road	Primary road name.	string	Maximum length: 47	
road-section	Road section.	string	Maximum length: 47	
room	Room number.	string	Maximum length: 47	
script	Script used to present the address information.	string	Maximum length: 47	
seat	Seat number.	string	Maximum length: 47	
street	Street.	string	Maximum length: 47	
street-name-post-mod	Street name post modifier.	string	Maximum length: 47	
street-name-pre-mod	Street name pre modifier.	string	Maximum length: 47	
street-suffix	Street suffix.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
sub-branch-road	Sub branch road name.	string	Maximum length: 47	
trailing-str-suffix	Trailing street suffix.	string	Maximum length: 47	
unit	Unit (apartment, suite).	string	Maximum length: 47	
zip	Postal/zip code.	string	Maximum length: 47	

config coordinates

Parameter	Description	Type	Size	Default								
altitude	Plus or minus floating point number. For example, 117.47.	string	Maximum length: 15									
altitude-unit	Configure the unit for which the altitude is to (m = meters, f = floors of a building).	option	-	m								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>m</i></td><td>set altitude unit meters</td></tr><tr><td><i>f</i></td><td>set altitude unit floors</td></tr></table>	Option	Description	<i>m</i>	set altitude unit meters	<i>f</i>	set altitude unit floors					
Option	Description											
<i>m</i>	set altitude unit meters											
<i>f</i>	set altitude unit floors											
datum	WGS84, NAD83, NAD83/MLLW.	option	-	WGS84								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>WGS84</i></td><td>set coordinates datum WGS84</td></tr><tr><td><i>NAD83</i></td><td>set coordinates datum NAD83</td></tr><tr><td><i>NAD83/MLLW</i></td><td>set coordinates datum NAD83/MLLW</td></tr></table>	Option	Description	<i>WGS84</i>	set coordinates datum WGS84	<i>NAD83</i>	set coordinates datum NAD83	<i>NAD83/MLLW</i>	set coordinates datum NAD83/MLLW			
Option	Description											
<i>WGS84</i>	set coordinates datum WGS84											
<i>NAD83</i>	set coordinates datum NAD83											
<i>NAD83/MLLW</i>	set coordinates datum NAD83/MLLW											
latitude	Floating point starting with +/- or ending with (N or S). For example, +/-16.67 or 16.67N.	string	Maximum length: 15									
longitude	Floating point starting with +/- or ending with (N or S). For example, +/-26.789 or 26.789E.	string	Maximum length: 15									
parent-key	Parent key name. Read-only.	string	Maximum length: 63									

config elin-number

Parameter	Description	Type	Size	Default
elin-num	Configure ELIN callback number.	string	Maximum length: 31	
parent-key	Parent key name. Read-only.	string	Maximum length: 63	

config switch-controller mac-policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure MAC policy to be applied on the managed FortiSwitch devices through NAC device.

```
config switch-controller mac-policy
    Description: Configure MAC policy to be applied on the managed FortiSwitch devices through NAC
    device.
    edit <name>
        set bounce-port-duration {integer}
        set bounce-port-link [disable|enable]
        set count [disable|enable]
        set description {string}
        set fortalink {string}
        set poe-reset [disable|enable]
        set traffic-policy {string}
```

```

        set vlan {string}
    next
end

```

config switch-controller mac-policy

Parameter	Description	Type	Size	Default
bounce-port-duration	Bounce duration in seconds of a switch port where this mac-policy is applied.	integer	Minimum value: 1 Maximum value: 30	5
bounce-port-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.	option	-	enable
	Option	Description		
	disable	Disable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.		
	enable	Enable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.		
count	Enable/disable packet count on the NAC device.	option	-	disable
	Option	Description		
	disable	Enable packet count on the NAC device.		
	enable	Disable packet count on the NAC device.		
description	Description for the MAC policy.	string	Maximum length: 63	
fortilink	FortiLink interface for which this MAC policy belongs to.	string	Maximum length: 15	
name	MAC policy name.	string	Maximum length: 63	
poe-reset	Enable/disable POE reset of a switch port where this mac-policy is applied.	option	-	disable
	Option	Description		
	disable	Disable POE reset of a switch port where this mac-policy is applied.		
	enable	Enable POE reset of a switch port where this mac-policy is applied.		
traffic-policy	Traffic policy to be applied when using this MAC policy.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
vlan	Ingress traffic VLAN assignment for the MAC address matching this MAC policy.	string	Maximum length: 15	

config switch-controller managed-switch



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R. It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch devices that are managed by this FortiGate.

```
config switch-controller managed-switch
  Description: Configure FortiSwitch devices that are managed by this FortiGate.
  edit <switch-id>
    config 802-1X-settings
      Description: Configuration method to edit FortiSwitch 802.1X global settings.
      set link-down-auth [set-unauth|no-action]
      set local-override [enable|disable]
      set mab-reauth [disable|enable]
      set mac-called-station-delimiter [colon|hyphen|...]
      set mac-calling-station-delimiter [colon|hyphen|...]
      set mac-case [lowercase|uppercase]
      set mac-password-delimiter [colon|hyphen|...]
      set mac-username-delimiter [colon|hyphen|...]
      set max-reauth-attempt {integer}
      set reauth-period {integer}
      set tx-period {integer}
```

```

end
set access-profile {string}
config custom-command
    Description: Configuration method to edit FortiSwitch commands to be pushed to this
FortiSwitch device upon rebooting the FortiGate switch controller or the FortiSwitch.
    edit <command-entry>
        set command-name {string}
    next
end
set delayed-restart-trigger {integer}
set description {string}
set dhcp-server-access-list [global|enable|...]
config dhcp-snooping-static-client
    Description: Configure FortiSwitch DHCP snooping static clients.
    edit <name>
        set ip {ipv4-address}
        set mac {mac-address}
        set port {string}
        set vlan {string}
    next
end
set directly-connected {integer}
set dynamic-capability {user}
set dynamically-discovered {integer}
set firmware-provision [enable|disable]
set firmware-provision-latest [disable|once]
set firmware-provision-version {string}
set flow-identity {user}
set fsw-wan1-admin [discovered|disable|...]
set fsw-wan1-peer {string}
config igmp-snooping
    Description: Configure FortiSwitch IGMP snooping global settings.
    set aging-time {integer}
    set flood-unknown-multicast [enable|disable]
    set local-override [enable|disable]
    config vlans
        Description: Configure IGMP snooping VLAN.
        edit <vlan-name>
            set proxy [disable|enable|...]
            set querier [disable|enable]
            set querier-addr {ipv4-address}
            set version {integer}
        next
    end
end
config ip-source-guard
    Description: IP source guard.
    edit <port>
        config binding-entry
            Description: IP and MAC address configuration.
            edit <entry-name>
                set ip {ipv4-address-any}

```



```

        set mac {mac-address}
    next
end
    set description {string}
next
end
set l3-discovered {integer}
set max-allowed-trunk-members {integer}
set mclag-igmp-snooping-aware [enable|disable]
set mgmt-mode {integer}
config mirror
    Description: Configuration method to edit FortiSwitch packet mirror.
    edit <name>
        set dst {string}
        set src-egress <name1>, <name2>, ...
        set src-ingress <name1>, <name2>, ...
        set status [active|inactive]
        set switching-packet [enable|disable]
    next
end
set override-snmp-community [enable|disable]
set override-snmp-sysinfo [disable|enable]
set override-snmp-trap-threshold [enable|disable]
set override-snmp-user [enable|disable]
set owner-vdom {string}
set poe-detection-type {integer}
set poe-pre-standard-detection [enable|disable]
config ports
    Description: Managed-switch port list.
    edit <port-name>
        set access-mode [dynamic|nac|...]
        set acl-group <name1>, <name2>, ...
        set aggregator-mode [bandwidth|count]
        set allow-arp-monitor [disable|enable]
        set allowed-vlans <vlan-name1>, <vlan-name2>, ...
        set allowed-vlans-all [enable|disable]
        set arp-inspection-trust [untrusted|trusted]
        set authenticated-port {integer}
        set bundle [enable|disable]
        set description {string}
        config dhcp-snoop-option82-override
            Description: Configure DHCP snooping option 82 override.
            edit <vlan-name>
                set circuit-id {string}
                set remote-id {string}
            next
        end
        set dhcp-snoop-option82-trust [enable|disable]
        set dhcp-snooping [untrusted|trusted]
        set discard-mode [none|all-untagged|...]
        set edge-port [enable|disable]
        set encrypted-port {integer}
    
```

```
set export-to {string}
set export-to-pool {string}
set fallback-port {string}
set fec-capable {integer}
set fec-state [disabled|c174|...]
set fgt-peer-device-name {string}
set fgt-peer-port-name {string}
set fiber-port {integer}
set flags {integer}
set flap-duration {integer}
set flap-rate {integer}
set flap-timeout {integer}
set flapguard [enable|disable]
set flow-control [disable|tx|...]
set fortilink-port {integer}
set fortiswitch-acls <id1>, <id2>, ...
set igmp-snooping-flood-reports [enable|disable]
set interface-tags <tag-name1>, <tag-name2>, ...
set ip-source-guard [disable|enable]
set isl-local-trunk-name {string}
set isl-peer-device-name {string}
set isl-peer-device-sn {string}
set isl-peer-port-name {string}
set lacp-speed [slow|fast]
set learning-limit {integer}
set lldp-profile {string}
set lldp-status [disable|rx-only|...]
set log-mac-event [disable|enable]
set loop-guard [enabled|disabled]
set loop-guard-timeout {integer}
set mac-addr {mac-address}
set matched-dpp-intf-tags {string}
set matched-dpp-policy {string}
set max-bundle {integer}
set mcast-snooping-flood-traffic [enable|disable]
set mclag [enable|disable]
set mclag-icl-port {integer}
set media-type {string}
set member-withdrawal-behavior [forward|block]
set members <member-name1>, <member-name2>, ...
set min-bundle {integer}
set mode [static|lacp-passive|...]
set p2p-port {integer}
set packet-sample-rate {integer}
set packet-sampler [enabled|disabled]
set pause-meter {integer}
set pause-meter-resume [75%|50%|...]
set pd-capable {integer}
set poe-capable {integer}
set poe-max-power {string}
set poe-mode-bt-cabable {integer}
set poe-port-mode [ieee802-3af|ieee802-3at|...]
```

```

    set poe-port-power [normal|perpetual|...]
    set poe-port-priority [critical-priority|high-priority|...]
    set poe-pre-standard-detection [enable|disable]
    set poe-standard {string}
    set poe-status [enable|disable]
    set port-number {integer}
    set port-owner {string}
    set port-policy {string}
    set port-prefix-type {integer}
    set port-security-policy {string}
    set port-selection-criteria [src-mac|dst-mac|...]
    set ptp-policy {string}
    set ptp-status [disable|enable]
    set qnq {string}
    set qos-policy {string}
    set restricted-auth-port {integer}
    set rpvst-port [disabled|enabled]
    set sample-direction [tx|rx|...]
    set sflow-counter-interval {integer}
    set speed [10half|10full|...]
    set stacking-port {integer}
    set status [up|down]
    set sticky-mac [enable|disable]
    set storm-control-policy {string}
    set stp-bpdu-guard [enabled|disabled]
    set stp-bpdu-guard-timeout {integer}
    set stp-root-guard [enabled|disabled]
    set stp-state [enabled|disabled]
    set switch-id {string}
    set type [physical|trunk]
    set untagged-vlans <vlan-name1>, <vlan-name2>, ...
    set vlan {string}
next
end
set pre-provisioned {integer}
set ptp-profile {string}
set ptp-status [disable|enable]
set purdue-level [1|1.5|...]
set qos-drop-policy [taildrop|random-early-detection]
set qos-red-probability {integer}
set radius-nas-ip {ipv4-address}
set radius-nas-ip-override [disable|enable]
config remote-log
    Description: Configure logging by FortiSwitch device to a remote syslog server.
    edit <name>
        set csv [enable|disable]
        set facility [kernel|user|...]
        set port {integer}
        set server {string}
        set severity [emergency|alert|...]
        set status [enable|disable]
    next

```

```

end
set route-offload [disable|enable]
set route-offload-mclag [disable|enable]
config route-offload-router
    Description: Configure route offload MCLAG IP address.
    edit <vlan-name>
        set router-ip {ipv4-address}
    next
end
set sn {string}
config snmp-community
    Description: Configuration method to edit Simple Network Management Protocol (SNMP)
communities.
    edit <id>
        set events {option1}, {option2}, ...
        config hosts
            Description: Configure IPv4 SNMP managers (hosts).
            edit <id>
                set ip {user}
            next
        end
        set name {string}
        set query-v1-port {integer}
        set query-v1-status [disable|enable]
        set query-v2c-port {integer}
        set query-v2c-status [disable|enable]
        set status [disable|enable]
        set trap-v1-lport {integer}
        set trap-v1-rport {integer}
        set trap-v1-status [disable|enable]
        set trap-v2c-lport {integer}
        set trap-v2c-rport {integer}
        set trap-v2c-status [disable|enable]
    next
end
config snmp-sysinfo
    Description: Configuration method to edit Simple Network Management Protocol (SNMP)
system info.
    set contact-info {string}
    set description {string}
    set engine-id {string}
    set location {string}
    set status [disable|enable]
end
config snmp-trap-threshold
    Description: Configuration method to edit Simple Network Management Protocol (SNMP)
trap threshold values.
    set trap-high-cpu-threshold {integer}
    set trap-log-full-threshold {integer}
    set trap-low-memory-threshold {integer}
end
config snmp-user

```

```

Description: Configuration method to edit Simple Network Management Protocol (SNMP)
users.
edit <name>
    set auth-proto [md5|sha1|...]
    set auth-pwd {password}
    set priv-proto [aes128|aes192|...]
    set priv-pwd {password}
    set queries [disable|enable]
    set query-port {integer}
    set security-level [no-auth-no-priv|auth-no-priv|...]
next
end
set staged-image-version {string}
config static-mac
    Description: Configuration method to edit FortiSwitch Static and Sticky MAC.
    edit <id>
        set description {string}
        set interface {string}
        set mac {mac-address}
        set type [static|sticky]
        set vlan {string}
    next
end
config storm-control
    Description: Configuration method to edit FortiSwitch storm control for measuring
traffic activity using data rates to prevent traffic disruption.
    set broadcast [enable|disable]
    set local-override [enable|disable]
    set rate {integer}
    set unknown-multicast [enable|disable]
    set unknown-unicast [enable|disable]
end
config stp-instance
    Description: Configuration method to edit Spanning Tree Protocol (STP) instances.
    edit <id>
        set priority [0|4096|...]
    next
end
config stp-settings
    Description: Configuration method to edit Spanning Tree Protocol (STP) settings used
to prevent bridge loops.
    set forward-time {integer}
    set hello-time {integer}
    set local-override [enable|disable]
    set max-age {integer}
    set max-hops {integer}
    set name {string}
    set pending-timer {integer}
    set revision {integer}
end
set switch-device-tag {string}
set switch-dhcp_opt43_key {string}

```

```

    config switch-log
        Description: Configuration method to edit FortiSwitch logging settings (logs are
transferred to and inserted into the FortiGate event log).
        set local-override [enable|disable]
        set severity [emergency|alert|...]
        set status [enable|disable]
    end
    set switch-profile {string}
    set tdr-supported {string}
    set tunnel-discovered {integer}
    set type [virtual|physical]
    set version {integer}
    config vlan
        Description: Configure VLAN assignment priority.
        edit <vlan-name>
            set assignment-priority {integer}
        next
    end
next
end

```

config switch-controller managed-switch

Parameter	Description	Type	Size	Default								
access-profile	FortiSwitch access profile.	string	Maximum length: 31	default								
delayed-restart-trigger	Delayed restart triggered for this FortiSwitch.	integer	Minimum value: 0 Maximum value: 255	0								
description	Description.	string	Maximum length: 63									
dhcp-server-access-list	DHCP snooping server access list.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>global</td><td>Use global setting for DHCP snooping server access list.</td></tr><tr><td>enable</td><td>Override global setting and enable DHCP server access list.</td></tr><tr><td>disable</td><td>Override global setting and disable DHCP server access list.</td></tr></table>				Option	Description	global	Use global setting for DHCP snooping server access list.	enable	Override global setting and enable DHCP server access list.	disable	Override global setting and disable DHCP server access list.
	Option	Description										
	global	Use global setting for DHCP snooping server access list.										
	enable	Override global setting and enable DHCP server access list.										
disable	Override global setting and disable DHCP server access list.											
directly-connected	Directly connected FortiSwitch. Read-only.	integer	Minimum value: 0 Maximum value: 1	0								

Parameter	Description	Type	Size	Default						
dynamic-capability	List of features this FortiSwitch supports (not configurable) that is sent to the FortiGate device for subsequent configuration initiated by the FortiGate device.	user	Not Specified	0x0000000000000000000000000000000000						
dynamically-discovered	Dynamically discovered FortiSwitch. Read-only.	integer	Minimum value: 0 Maximum value: 1	0						
firmware-provision	Enable/disable provisioning of firmware to FortiSwitches on join connection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable firmware-provision.</td></tr><tr><td>disable</td><td>Disable firmware-provision.</td></tr></table>				Option	Description	enable	Enable firmware-provision.	disable	Disable firmware-provision.
Option	Description									
enable	Enable firmware-provision.									
disable	Disable firmware-provision.									
firmware-provision-latest	Enable/disable one-time automatic provisioning of the latest firmware version.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not automatically provision the latest available firmware.</td></tr><tr><td>once</td><td>Automatically attempt a one-time upgrade to the latest available firmware version.</td></tr></table>				Option	Description	disable	Do not automatically provision the latest available firmware.	once	Automatically attempt a one-time upgrade to the latest available firmware version.
Option	Description									
disable	Do not automatically provision the latest available firmware.									
once	Automatically attempt a one-time upgrade to the latest available firmware version.									
firmware-provision-version	Firmware version to provision to this FortiSwitch on bootup (major.minor.build, i.e. 6.2.1234).	string	Maximum length: 35							

Parameter	Description	Type	Size	Default								
flow-identity	Flow-tracking netflow ipfix switch identity in hex format(00000000-FFFFFFFF default=0).	user	Not Specified	00000000								
fsw-wan1-admin	FortiSwitch WAN1 admin status; enable to authorize the FortiSwitch as a managed switch.	option	-	discovered								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>discovered</td><td>Link waiting to be authorized.</td></tr><tr><td>disable</td><td>Link unauthorized.</td></tr><tr><td>enable</td><td>Link authorized.</td></tr></table>				Option	Description	discovered	Link waiting to be authorized.	disable	Link unauthorized.	enable	Link authorized.
Option	Description											
discovered	Link waiting to be authorized.											
disable	Link unauthorized.											
enable	Link authorized.											
fsw-wan1-peer	FortiSwitch WAN1 peer port.	string	Maximum length: 35									
l3-discovered	Layer 3 management discovered. Read-only.	integer	Minimum value: 0 Maximum value: 1	0								
max-allowed-trunk-members	FortiSwitch maximum allowed trunk members.	integer	Minimum value: 0 Maximum value: 255	0								
mclag-igmp-snooping-aware	Enable/disable MCLAG IGMP-snooping awareness.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable MCLAG IGMP-snooping awareness.</td></tr><tr><td>disable</td><td>Disable MCLAG IGMP-snooping awareness.</td></tr></table>				Option	Description	enable	Enable MCLAG IGMP-snooping awareness.	disable	Disable MCLAG IGMP-snooping awareness.		
Option	Description											
enable	Enable MCLAG IGMP-snooping awareness.											
disable	Disable MCLAG IGMP-snooping awareness.											
mgmt-mode	FortiLink management mode.	integer	Minimum value: 0 Maximum value: 255	0								

Parameter	Description	Type	Size	Default						
override-snmpp-community	Enable/disable overriding the global SNMP communities.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the global SNMP communities.</td></tr><tr><td>disable</td><td>Use the global SNMP communities.</td></tr></table>	Option	Description	enable	Override the global SNMP communities.	disable	Use the global SNMP communities.			
Option	Description									
enable	Override the global SNMP communities.									
disable	Use the global SNMP communities.									
override-snmpp-sysinfo	Enable/disable overriding the global SNMP system information.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Use the global SNMP system information.</td></tr><tr><td>enable</td><td>Override the global SNMP system information.</td></tr></table>	Option	Description	disable	Use the global SNMP system information.	enable	Override the global SNMP system information.			
Option	Description									
disable	Use the global SNMP system information.									
enable	Override the global SNMP system information.									
override-snmpp-trap-threshold	Enable/disable overriding the global SNMP trap threshold values.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the global SNMP trap threshold values.</td></tr><tr><td>disable</td><td>Use the global SNMP trap threshold values.</td></tr></table>	Option	Description	enable	Override the global SNMP trap threshold values.	disable	Use the global SNMP trap threshold values.			
Option	Description									
enable	Override the global SNMP trap threshold values.									
disable	Use the global SNMP trap threshold values.									
override-snmpp-user	Enable/disable overriding the global SNMP users.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the global SNMPv3 users.</td></tr><tr><td>disable</td><td>Use the global SNMPv3 users.</td></tr></table>	Option	Description	enable	Override the global SNMPv3 users.	disable	Use the global SNMPv3 users.			
Option	Description									
enable	Override the global SNMPv3 users.									
disable	Use the global SNMPv3 users.									
owner-vdom	VDOM which owner of port belongs to.	string	Maximum length: 31							
poe-detection-type	PoE detection type for FortiSwitch.	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PoE pre-standard detection.		
	<i>disable</i>	Disable PoE pre-standard detection.		
pre-provisioned	Pre-provisioned managed switch.	integer	Minimum value: 0 Maximum value: 255	0
ptp-profile	PTP profile configuration.	string	Maximum length: 63	default
ptp-status	Enable/disable PTP profile on this FortiSwitch.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable PTP profile.		
	<i>enable</i>	Enable PTP profile.		
purdue-level	Purdue Level of this FortiSwitch.	option	-	3
	Option	Description		
	1	Level 1 - Basic Control		
	1.5	Level 1.5		
	2	Level 2 - Area Supervisory Control		
	2.5	Level 2.5		
	3	Level 3 - Operations & Control		
	3.5	Level 3.5		
	4	Level 4 - Business Planning & Logistics		
	5	Level 5 - Enterprise Network		
	5.5	Level 5.5		
qos-drop-policy	Set QoS drop-policy.	option	-	taildrop

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>taildrop</i>	Taildrop policy.		
	<i>random-early-detection</i>	Random early detection drop policy.		
qos-red-probability	Set QoS RED/WRED drop probability.	integer	Minimum value: 0 Maximum value: 100	12
radius-nas-ip	NAS-IP address.	ipv4-address	Not Specified	0.0.0.0
radius-nas-ip-override	Use locally defined NAS-IP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable radius-nas-ip-override.		
	<i>enable</i>	Enable radius-nas-ip-override.		
route-offload	Enable/disable route offload on this FortiSwitch.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable route offload.		
	<i>enable</i>	Enable route offload.		
route-offload-mclag	Enable/disable route offload MCLAG on this FortiSwitch.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable route offload MCLAG.		
	<i>enable</i>	Enable route offload MCLAG.		
sn	Managed-switch serial number.	string	Maximum length: 16	
staged-image-version	Staged image version for FortiSwitch.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default						
switch-device-tag	User definable label/tag.	string	Maximum length: 32							
switch-dhcp_opt43_key	DHCP option43 key.	string	Maximum length: 63							
switch-id	Managed-switch name.	string	Maximum length: 16							
switch-profile	FortiSwitch profile.	string	Maximum length: 35	default						
tdr-supported	TDR supported. Read-only.	string	Maximum length: 31							
tunnel-discovered	SOCKS tunnel management discovered. Read-only.	integer	Minimum value: 0 Maximum value: 1	0						
type	Indication of switch type, physical or virtual.	option	-	physical						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>virtual</i></td><td>Switch is of type virtual.</td></tr><tr><td><i>physical</i></td><td>Switch is of type physical.</td></tr></table>				Option	Description	<i>virtual</i>	Switch is of type virtual.	<i>physical</i>	Switch is of type physical.
Option	Description									
<i>virtual</i>	Switch is of type virtual.									
<i>physical</i>	Switch is of type physical.									
version	FortiSwitch version.	integer	Minimum value: 0 Maximum value: 255	0						

config 802-1X-settings

Parameter	Description	Type	Size	Default
link-down-auth	Authentication state to set if a link is down.	option	-	set-unauth
	Option	Description		
	<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.		
	<i>no-action</i>	Interface reauthentication is not needed.		
local-override	Enable to override global 802.1X settings on individual FortiSwitches.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Override global 802.1X settings.		
	<i>disable</i>	Use global 802.1X settings.		
mab-reauth	Enable or disable MAB reauthentication settings.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable MAB re-authentication settings.		
	<i>enable</i>	Enable MAB re-authentication settings.		
mac-called-station-delimiter	MAC called station delimiter (default = hyphen).	option	-	hyphen
	Option	Description		
	<i>colon</i>	Use colon as delimiter for called station.		
	<i>hyphen</i>	Use hyphen as delimiter for called station.		
	<i>none</i>	No delimiter for called station.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for called station.		
mac-calling-station-delimiter	MAC calling station delimiter (default = hyphen).	option	-	hyphen
	Option	Description		
	<i>colon</i>	Use colon as delimiter for calling station.		
	<i>hyphen</i>	Use hyphen as delimiter for calling station.		
	<i>none</i>	No delimiter for calling station.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for calling station.		
mac-case	MAC case (default = lowercase).	option	-	lowercase
	Option	Description		
	<i>lowercase</i>	Use lowercase MAC.		
	<i>uppercase</i>	Use uppercase MAC.		
mac-password-delimiter	MAC authentication password delimiter (default = hyphen).	option	-	hyphen

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>colon</i>	Use colon as delimiter for MAC auth password.		
	<i>hyphen</i>	Use hyphen as delimiter for MAC auth password.		
	<i>none</i>	No delimiter for MAC auth password.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC auth password.		
mac-username-delimiter	MAC authentication username delimiter (default = hyphen).	option	-	hyphen
	Option	Description		
	<i>colon</i>	Use colon as delimiter for MAC auth username.		
	<i>hyphen</i>	Use hyphen as delimiter for MAC auth username.		
	<i>none</i>	No delimiter for MAC auth username.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC auth username.		
max-reauth-attempt	Maximum number of authentication attempts (0 - 15, default = 3).	integer	Minimum value: 0 Maximum value: 15	3
reauth-period	Reauthentication time interval (1 - 1440 min, default = 60, 0 = disable).	integer	Minimum value: 0 Maximum value: 1440	60
tx-period	802.1X Tx period (seconds, default=30).	integer	Minimum value: 12 Maximum value: 60	30

config custom-command

Parameter	Description	Type	Size	Default
command-entry	List of FortiSwitch commands.	string	Maximum length: 35	
command-name	Names of commands to be pushed to this FortiSwitch device, as configured under config switch-controller custom-command.	string	Maximum length: 35	

config dhcp-snooping-static-client

Parameter	Description	Type	Size	Default
ip	Client static IP address.	ipv4-address	Not Specified	0.0.0.0
mac	Client MAC address.	mac-address	Not Specified	00:00:00:00:00:00
name	Client name.	string	Maximum length: 35	
port	Interface name.	string	Maximum length: 15	
vlan	VLAN name.	string	Maximum length: 15	

config igmp-snooping

Parameter	Description	Type	Size	Default						
aging-time	Maximum time to retain a multicast snooping entry for which no packets have been seen (15 - 3600 sec, default = 300).	integer	Minimum value: 15 Maximum value: 3600	300						
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unknown multicast flooding.</td></tr><tr><td><i>disable</i></td><td>Disable unknown multicast flooding.</td></tr></table>	Option	Description	<i>enable</i>	Enable unknown multicast flooding.	<i>disable</i>	Disable unknown multicast flooding.			
Option	Description									
<i>enable</i>	Enable unknown multicast flooding.									
<i>disable</i>	Disable unknown multicast flooding.									
local-override	Enable/disable overriding the global IGMP snooping configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the global IGMP snooping configuration.</td></tr><tr><td><i>disable</i></td><td>Use the global IGMP snooping configuration.</td></tr></table>	Option	Description	<i>enable</i>	Override the global IGMP snooping configuration.	<i>disable</i>	Use the global IGMP snooping configuration.			
Option	Description									
<i>enable</i>	Override the global IGMP snooping configuration.									
<i>disable</i>	Use the global IGMP snooping configuration.									

config vlans

Parameter	Description	Type	Size	Default
proxy	IGMP snooping proxy for the VLAN interface.	option	-	global

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable IGMP snooping proxy on VLAN interface.		
	<i>enable</i>	Enable IGMP snooping proxy on VLAN interface.		
	<i>global</i>	Use global setting for IGMP snooping proxy on VLAN interface.		
querier	Enable/disable IGMP snooping querier for the VLAN interface.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable IGMP snooping querier on VLAN interface.		
	<i>enable</i>	Enable IGMP snooping querier on VLAN interface.		
querier-addr	IGMP snooping querier address.	ipv4-address	Not Specified	0.0.0.0
version	IGMP snooping querying version.	integer	Minimum value: 2 Maximum value: 3	2
vlan-name	List of FortiSwitch VLANs.	string	Maximum length: 15	default

config ip-source-guard

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
port	Ingress interface to which source guard is bound.	string	Maximum length: 15	

config binding-entry

Parameter	Description	Type	Size	Default
entry-name	Configure binding pair.	string	Maximum length: 16	
ip	Source IP for this rule.	ipv4-address-any	Not Specified	0.0.0.0
mac	MAC address for this rule.	mac-address	Not Specified	00:00:00:00:00:00

config mirror

Parameter	Description	Type	Size	Default						
dst	Destination port.	string	Maximum length: 63							
name	Mirror name.	string	Maximum length: 63							
src-egress <name>	Source egress interfaces. Interface name.	string	Maximum length: 79							
src-ingress <name>	Source ingress interfaces. Interface name.	string	Maximum length: 79							
status	Active/inactive mirror configuration.	option	-	inactive						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Activate mirror configuration.</td></tr><tr><td><i>inactive</i></td><td>Deactivate mirror configuration.</td></tr></table>				Option	Description	<i>active</i>	Activate mirror configuration.	<i>inactive</i>	Deactivate mirror configuration.
Option	Description									
<i>active</i>	Activate mirror configuration.									
<i>inactive</i>	Deactivate mirror configuration.									
switching-packet	Enable/disable switching functionality when mirroring.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable switching functionality when mirroring.</td></tr><tr><td><i>disable</i></td><td>Disable switching functionality when mirroring.</td></tr></table>				Option	Description	<i>enable</i>	Enable switching functionality when mirroring.	<i>disable</i>	Disable switching functionality when mirroring.
Option	Description									
<i>enable</i>	Enable switching functionality when mirroring.									
<i>disable</i>	Disable switching functionality when mirroring.									

config ports

Parameter	Description	Type	Size	Default
access-mode	Access mode of the port.	option	-	static
	Option	Description		
	<i>dynamic</i>	Dynamic mode.		
	<i>nac</i>	NAC mode.		
	<i>static</i>	Static mode.		
acl-group <name>	ACL groups on this port. ACL group name.	string	Maximum length: 79	
aggregator-mode	LACP member select mode.	option	-	bandwidth

Parameter	Description	Type	Size	Default
	Option Description			
	<i>bandwidth</i>	Member selection based on largest total bandwidth of links of similar speed.		
	<i>count</i>	Member selection based on largest count of similar link speed.		
allow-arp-monitor	Enable/Disable allow ARP monitor.	option	-	disable
	Option Description			
	<i>disable</i>	Disable allow ARP monitor.		
	<i>enable</i>	Enable allow ARP monitor.		
allowed-vlans <vlan-name>	Configure switch port tagged VLANs. VLAN name.	string	Maximum length: 79	
allowed-vlans-all	Enable/disable all defined vlans on this port.	option	-	disable
	Option Description			
	<i>enable</i>	Enable all defined VLANs on this port.		
	<i>disable</i>	Disable all defined VLANs on this port.		
arp-inspection-trust	Trusted or untrusted dynamic ARP inspection.	option	-	untrusted
	Option Description			
	<i>untrusted</i>	Untrusted dynamic ARP inspection.		
	<i>trusted</i>	Trusted dynamic ARP inspection.		
authenticated-port	Peer to Peer Authenticated port. Read-only.	integer	Minimum value: 0 Maximum value: 1	0
bundle	Enable/disable Link Aggregation Group (LAG) bundling for non-FortiLink interfaces.	option	-	disable
	Option Description			
	<i>enable</i>	Enable bundling.		
	<i>disable</i>	Disable bundling.		

Parameter	Description	Type	Size	Default								
description	Description for port.	string	Maximum length: 63									
dhcp-snoop-option82-trust	Enable/disable allowance of DHCP with option-82 on untrusted interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowance of DHCP with option-82 on untrusted interface.</td></tr><tr><td><i>disable</i></td><td>Disable allowance of DHCP with option-82 on untrusted interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.	<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.					
Option	Description											
<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.											
<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.											
dhcp-snooping	Trusted or untrusted DHCP-snooping interface.	option	-	untrusted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>untrusted</i></td><td>Untrusted DHCP snooping interface.</td></tr><tr><td><i>trusted</i></td><td>Trusted DHCP snooping interface.</td></tr></table>	Option	Description	<i>untrusted</i>	Untrusted DHCP snooping interface.	<i>trusted</i>	Trusted DHCP snooping interface.					
Option	Description											
<i>untrusted</i>	Untrusted DHCP snooping interface.											
<i>trusted</i>	Trusted DHCP snooping interface.											
discard-mode	Configure discard mode for port.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Discard disabled.</td></tr><tr><td><i>all-untagged</i></td><td>Discard all frames that are untagged.</td></tr><tr><td><i>all-tagged</i></td><td>Discard all frames that are tagged.</td></tr></table>	Option	Description	<i>none</i>	Discard disabled.	<i>all-untagged</i>	Discard all frames that are untagged.	<i>all-tagged</i>	Discard all frames that are tagged.			
Option	Description											
<i>none</i>	Discard disabled.											
<i>all-untagged</i>	Discard all frames that are untagged.											
<i>all-tagged</i>	Discard all frames that are tagged.											
edge-port	Enable/disable this interface as an edge port, bridging connections between workstations and/or computers.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this interface as an edge port.</td></tr><tr><td><i>disable</i></td><td>Disable this interface as an edge port.</td></tr></table>	Option	Description	<i>enable</i>	Enable this interface as an edge port.	<i>disable</i>	Disable this interface as an edge port.					
Option	Description											
<i>enable</i>	Enable this interface as an edge port.											
<i>disable</i>	Disable this interface as an edge port.											
encrypted-port	Peer to Peer Encrypted port. Read-only.	integer	Minimum value: 0 Maximum value: 1									
export-to	Export managed-switch port to a tenant VDOM.	string	Maximum length: 31									
export-to-pool	Switch controller export port to pool-list.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default										
fallback-port	LACP fallback port.	string	Maximum length: 79											
fec-capable	FEC capable.	integer	Minimum value: 0 0 Maximum value: 1											
fec-state	State of forward error correction.	option	-	detect-by-module										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>Disable forward error correction.</td></tr><tr><td><i>cl74</i></td><td>Enable Clause 74 FC-FEC, which only applies to 25Gbps.</td></tr><tr><td><i>cl91</i></td><td>Enable Clause 91 RS-FEC, which only applies to 100Gbps.</td></tr><tr><td><i>detect-by-module</i></td><td>FEC supported by module.</td></tr></table>				Option	Description	<i>disabled</i>	Disable forward error correction.	<i>cl74</i>	Enable Clause 74 FC-FEC, which only applies to 25Gbps.	<i>cl91</i>	Enable Clause 91 RS-FEC, which only applies to 100Gbps.	<i>detect-by-module</i>	FEC supported by module.
Option	Description													
<i>disabled</i>	Disable forward error correction.													
<i>cl74</i>	Enable Clause 74 FC-FEC, which only applies to 25Gbps.													
<i>cl91</i>	Enable Clause 91 RS-FEC, which only applies to 100Gbps.													
<i>detect-by-module</i>	FEC supported by module.													
fgt-peer-device-name	FGT peer device name. Read-only.	string	Maximum length: 16											
fgt-peer-port-name	FGT peer port name. Read-only.	string	Maximum length: 15											
fiber-port	Fiber-port. Read-only.	integer	Minimum value: 0 0 Maximum value: 1											
flags	Port properties flags. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295											
flap-duration	Period over which flap events are calculated (seconds).	integer	Minimum value: 5 5 Maximum value: 300	30										
flap-rate	Number of stage change events needed within flap-duration.	integer	Minimum value: 1 1 Maximum value: 30	5										
flap-timeout	Flap guard disabling protection (min).	integer	Minimum value: 0 0 Maximum value: 120	0										
flapguard	Enable/disable flap guard.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FlapGuard for this port.</td></tr><tr><td><i>disable</i></td><td>Disable FlapGuard for this port.</td></tr></table>				Option	Description	<i>enable</i>	Enable FlapGuard for this port.	<i>disable</i>	Disable FlapGuard for this port.				
Option	Description													
<i>enable</i>	Enable FlapGuard for this port.													
<i>disable</i>	Disable FlapGuard for this port.													

Parameter	Description	Type	Size	Default										
flow-control	Flow control direction.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable flow control.</td></tr><tr><td>tx</td><td>Enable flow control for transmission pause control frames.</td></tr><tr><td>rx</td><td>Enable flow control for receive pause control frames.</td></tr><tr><td>both</td><td>Enable flow control for both transmission and receive pause control frames.</td></tr></table>	Option	Description	disable	Disable flow control.	tx	Enable flow control for transmission pause control frames.	rx	Enable flow control for receive pause control frames.	both	Enable flow control for both transmission and receive pause control frames.			
	Option	Description												
	disable	Disable flow control.												
	tx	Enable flow control for transmission pause control frames.												
	rx	Enable flow control for receive pause control frames.												
both	Enable flow control for both transmission and receive pause control frames.													
fortilink-port	FortiLink uplink port. Read-only.	integer	Minimum value: 0 Maximum value: 1											
fortiswitch-acls <id>	ACLs on this port. ACL ID.	integer	Minimum value: 0 Maximum value: 4294967295											
igmp-snooping-flood-reports	Enable/disable flooding of IGMP reports to this interface when igmp-snooping enabled.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable flooding of IGMP snooping reports to this interface.</td></tr><tr><td>disable</td><td>Disable flooding of IGMP snooping reports to this interface.</td></tr></table>	Option	Description	enable	Enable flooding of IGMP snooping reports to this interface.	disable	Disable flooding of IGMP snooping reports to this interface.							
	Option	Description												
	enable	Enable flooding of IGMP snooping reports to this interface.												
disable	Disable flooding of IGMP snooping reports to this interface.													
interface-tags <tag-name>	Tag(s) associated with the interface for various features including virtual port pool, dynamic port policy. FortiSwitch port tag name when exported to a virtual port pool or matched to dynamic port policy.	string	Maximum length: 63											
ip-source-guard	Enable/disable IP source guard.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable IP source guard.</td></tr><tr><td>enable</td><td>Enable IP source guard.</td></tr></table>	Option	Description	disable	Disable IP source guard.	enable	Enable IP source guard.							
	Option	Description												
	disable	Disable IP source guard.												
enable	Enable IP source guard.													
isl-local-trunk-name	ISL local trunk name. Read-only.	string	Maximum length: 15											

Parameter	Description	Type	Size	Default										
isl-peer-device-name	ISL peer device name. Read-only.	string	Maximum length: 16											
isl-peer-device-sn	ISL peer device serial number. Read-only.	string	Maximum length: 16											
isl-peer-port-name	ISL peer port name. Read-only.	string	Maximum length: 15											
lacp-speed	End Link Aggregation Control Protocol (LACP) messages every 30 seconds (slow) or every second (fast).	option	-	slow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>slow</td><td>Send LACP message every 30 seconds.</td></tr><tr><td>fast</td><td>Send LACP message every second.</td></tr></table>				Option	Description	slow	Send LACP message every 30 seconds.	fast	Send LACP message every second.				
Option	Description													
slow	Send LACP message every 30 seconds.													
fast	Send LACP message every second.													
learning-limit	Limit the number of dynamic MAC addresses on this Port (1 - 128, 0 = no limit, default).	integer	Minimum value: 0 0 Maximum value: 128											
lldp-profile	LLDP port TLV profile.	string	Maximum length: 63	default-auto-isl										
lldp-status	LLDP transmit and receive status.	option	-	tx-rx										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable LLDP TX and RX.</td></tr><tr><td>rx-only</td><td>Enable LLDP as RX only.</td></tr><tr><td>tx-only</td><td>Enable LLDP as TX only.</td></tr><tr><td>tx-rx</td><td>Enable LLDP TX and RX.</td></tr></table>				Option	Description	disable	Disable LLDP TX and RX.	rx-only	Enable LLDP as RX only.	tx-only	Enable LLDP as TX only.	tx-rx	Enable LLDP TX and RX.
Option	Description													
disable	Disable LLDP TX and RX.													
rx-only	Enable LLDP as RX only.													
tx-only	Enable LLDP as TX only.													
tx-rx	Enable LLDP TX and RX.													
log-mac-event	Enable/disable logging for dynamic MAC address events.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable log MAC event for this interface.</td></tr><tr><td>enable</td><td>Enable log MAC event for this interface.</td></tr></table>				Option	Description	disable	Disable log MAC event for this interface.	enable	Enable log MAC event for this interface.				
Option	Description													
disable	Disable log MAC event for this interface.													
enable	Enable log MAC event for this interface.													
loop-guard	Enable/disable loop-guard on this interface, an STP optimization used to prevent network loops.	option	-	disabled										

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enabled</i></td><td>Enable loop-guard on this interface.</td></tr><tr><td><i>disabled</i></td><td>Disable loop-guard on this interface.</td></tr></table>	Option	Description	<i>enabled</i>	Enable loop-guard on this interface.	<i>disabled</i>	Disable loop-guard on this interface.			
	Option	Description								
	<i>enabled</i>	Enable loop-guard on this interface.								
<i>disabled</i>	Disable loop-guard on this interface.									
loop-guard-timeout	Loop-guard timeout (0 - 120 min, default = 45).	integer	Minimum value: 0 Maximum value: 120	45						
mac-addr	Port/Trunk MAC.	mac-address	Not Specified	00:00:00:00:00:00						
matched-dpp-intf-tags	Matched interface tags in the dynamic port policy.	string	Maximum length: 63							
matched-dpp-policy	Matched child policy in the dynamic port policy.	string	Maximum length: 63							
max-bundle	Maximum size of LAG bundle (1 - 24, default = 24).	integer	Minimum value: 1 Maximum value: 24	24						
mcast-snooping-flood-traffic	Enable/disable flooding of IGMP snooping traffic to this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable flooding of IGMP snooping traffic to this interface.</td></tr><tr><td><i>disable</i></td><td>Disable flooding of IGMP snooping traffic to this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable flooding of IGMP snooping traffic to this interface.	<i>disable</i>	Disable flooding of IGMP snooping traffic to this interface.			
	Option	Description								
	<i>enable</i>	Enable flooding of IGMP snooping traffic to this interface.								
<i>disable</i>	Disable flooding of IGMP snooping traffic to this interface.									
mclag	Enable/disable multi-chassis link aggregation (MCLAG).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MCLAG.</td></tr><tr><td><i>disable</i></td><td>Disable MCLAG.</td></tr></table>	Option	Description	<i>enable</i>	Enable MCLAG.	<i>disable</i>	Disable MCLAG.			
	Option	Description								
	<i>enable</i>	Enable MCLAG.								
<i>disable</i>	Disable MCLAG.									
mclag-icl-port	MCLAG-ICL port. Read-only.	integer	Minimum value: 0 Maximum value: 1	0						
media-type	Media type. Read-only.	string	Maximum length: 31							
member-withdrawal-behavior	Port behavior after it withdraws because of loss of control packets.	option	-	block						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward traffic.</td></tr><tr><td><i>block</i></td><td>Block traffic.</td></tr></table>	Option	Description	<i>forward</i>	Forward traffic.	<i>block</i>	Block traffic.					
	Option	Description										
	<i>forward</i>	Forward traffic.										
<i>block</i>	Block traffic.											
members <member-name>	Aggregated LAG bundle interfaces. Interface name from available options.	string	Maximum length: 79									
min-bundle	Minimum size of LAG bundle (1 - 24, default = 1).	integer	Minimum value: 1 Maximum value: 24									
mode	LACP mode: ignore and do not send control messages, or negotiate 802.3ad aggregation passively or actively.	option	-	static								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Static aggregation, do not send and ignore any control messages.</td></tr><tr><td><i>lacp-passive</i></td><td>Passively use LACP to negotiate 802.3ad aggregation.</td></tr><tr><td><i>lacp-active</i></td><td>Actively use LACP to negotiate 802.3ad aggregation.</td></tr></table>	Option	Description	<i>static</i>	Static aggregation, do not send and ignore any control messages.	<i>lacp-passive</i>	Passively use LACP to negotiate 802.3ad aggregation.	<i>lacp-active</i>	Actively use LACP to negotiate 802.3ad aggregation.			
	Option	Description										
	<i>static</i>	Static aggregation, do not send and ignore any control messages.										
	<i>lacp-passive</i>	Passively use LACP to negotiate 802.3ad aggregation.										
<i>lacp-active</i>	Actively use LACP to negotiate 802.3ad aggregation.											
p2p-port	General peer to peer tunnel port. Read-only.	integer	Minimum value: 0 Maximum value: 1									
packet-sample-rate	Packet sampling rate (0 - 99999 p/sec).	integer	Minimum value: 512 Maximum value: 99999									
packet-sampler	Enable/disable packet sampling on this interface.	option	-	disabled								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enabled</i></td><td>Enable packet sampling on this interface.</td></tr><tr><td><i>disabled</i></td><td>Disable packet sampling on this interface.</td></tr></table>	Option	Description	<i>enabled</i>	Enable packet sampling on this interface.	<i>disabled</i>	Disable packet sampling on this interface.					
	Option	Description										
	<i>enabled</i>	Enable packet sampling on this interface.										
<i>disabled</i>	Disable packet sampling on this interface.											
pause-meter	Configure ingress pause metering rate, in kbps (default = 0, disabled).	integer	Minimum value: 128 Maximum value: 2147483647	0								
pause-meter-resume	Resume threshold for resuming traffic on ingress port.	option	-	50%								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>75%</td><td>Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.</td></tr><tr><td>50%</td><td>Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.</td></tr><tr><td>25%</td><td>Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.</td></tr></table>	Option	Description	75%	Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.	50%	Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.	25%	Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.			
	Option	Description										
	75%	Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.										
	50%	Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.										
25%	Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.											
pd-capable	Powered device capable.	integer	Minimum value: 0 0 Maximum value: 1									
poe-capable	PoE capable.	integer	Minimum value: 0 0 Maximum value: 1									
poe-max-power	PoE maximum power. Read-only.	string	Maximum length: 35									
poe-mode-bt-cabable	PoE mode IEEE 802.3BT capable.	integer	Minimum value: 0 0 Maximum value: 1									
poe-port-mode	Configure PoE port mode.	option	-	ieee802-3at								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ieee802-3af</td><td>IEEE802.3 AF.</td></tr><tr><td>ieee802-3at</td><td>IEEE802.3 AT.</td></tr><tr><td>ieee802-3bt</td><td>IEEE802.3 BT.</td></tr></table>	Option	Description	ieee802-3af	IEEE802.3 AF.	ieee802-3at	IEEE802.3 AT.	ieee802-3bt	IEEE802.3 BT.			
	Option	Description										
	ieee802-3af	IEEE802.3 AF.										
	ieee802-3at	IEEE802.3 AT.										
ieee802-3bt	IEEE802.3 BT.											
poe-port-power	Configure PoE port power.	option	-	normal								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>normal</td><td>Power not delivered during boot.</td></tr><tr><td>perpetual</td><td>Power delivered during soft reboot.</td></tr><tr><td>perpetual-fast</td><td>Early power delivered during cold boot.</td></tr></table>	Option	Description	normal	Power not delivered during boot.	perpetual	Power delivered during soft reboot.	perpetual-fast	Early power delivered during cold boot.			
	Option	Description										
	normal	Power not delivered during boot.										
	perpetual	Power delivered during soft reboot.										
perpetual-fast	Early power delivered during cold boot.											
poe-port-priority	Configure PoE port priority.	option	-	low-priority								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>critical-priority</td><td>Critical Priority.</td></tr><tr><td>high-priority</td><td>High Priority.</td></tr></table>	Option	Description	critical-priority	Critical Priority.	high-priority	High Priority.					
	Option	Description										
	critical-priority	Critical Priority.										
high-priority	High Priority.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low-priority</i></td><td>Low Priority.</td></tr><tr><td><i>medium-priority</i></td><td>Medium Priority.</td></tr></table>	Option	Description	<i>low-priority</i>	Low Priority.	<i>medium-priority</i>	Medium Priority.			
	Option	Description								
	<i>low-priority</i>	Low Priority.								
<i>medium-priority</i>	Medium Priority.									
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PoE pre-standard detection.</td></tr><tr><td><i>disable</i></td><td>Disable PoE pre-standard detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable PoE pre-standard detection.	<i>disable</i>	Disable PoE pre-standard detection.			
	Option	Description								
	<i>enable</i>	Enable PoE pre-standard detection.								
<i>disable</i>	Disable PoE pre-standard detection.									
poe-standard	PoE standard supported. Read-only.	string	Maximum length: 63							
poe-status	Enable/disable PoE status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PoE status.</td></tr><tr><td><i>disable</i></td><td>Disable PoE status.</td></tr></table>	Option	Description	<i>enable</i>	Enable PoE status.	<i>disable</i>	Disable PoE status.			
	Option	Description								
	<i>enable</i>	Enable PoE status.								
<i>disable</i>	Disable PoE status.									
port-name	Switch port name.	string	Maximum length: 15							
port-number	Port number. Read-only.	integer	Minimum value: 0 1 Maximum value: 64							
port-owner	Switch port name.	string	Maximum length: 15							
port-policy	Switch controller dynamic port policy from available options.	string	Maximum length: 63							
port-prefix-type	Port prefix type. Read-only.	integer	Minimum value: 0 0 Maximum value: 1							
port-security-policy	Switch controller authentication policy to apply to this managed switch from available options.	string	Maximum length: 31							
port-selection-criteria	Algorithm for aggregate port selection.	option	-	src-dst-ip						

Parameter	Description	Type	Size	Default
	Option	Description		
	src-mac	Source MAC address.		
	dst-mac	Destination MAC address.		
	src-dst-mac	Source and destination MAC address.		
	src-ip	Source IP address.		
	dst-ip	Destination IP address.		
	src-dst-ip	Source and destination IP address.		
ptp-policy	PTP policy configuration.	string	Maximum length: 63	default
ptp-status	Enable/disable PTP policy on this FortiSwitch port.	option	-	enable
	Option	Description		
	disable	Disable PTP policy.		
	enable	Enable PTP policy.		
qnq	802.1AD VLANs in the VDom.	string	Maximum length: 15	
qos-policy	Switch controller QoS policy from available options.	string	Maximum length: 63	default
restricted-auth-port	Peer to Peer Restricted Authenticated port. Read-only.	integer	Minimum value: 0 0 Maximum value: 1	0
rpvst-port	Enable/disable inter-operability with rapid PVST on this interface.	option	-	disabled
	Option	Description		
	disabled	Disable inter-operability with rapid PVST on this interface.		
	enabled	Enable inter-operability with rapid PVST on this interface.		
sample-direction	Packet sampling direction.	option	-	both
	Option	Description		
	tx	Monitor transmitted traffic.		
	rx	Monitor received traffic.		
	both	Monitor transmitted and received traffic.		

Parameter	Description	Type	Size	Default
sflow-counter-interval	sFlow sampling counter polling interval in seconds (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0
speed	Switch port speed; default and available settings depend on hardware.	option	-	auto

Option	Description
<i>10half</i>	10M half-duplex.
<i>10full</i>	10M full-duplex.
<i>100half</i>	100M half-duplex.
<i>100full</i>	100M full-duplex.
<i>1000full</i>	1G full-duplex
<i>10000full</i>	10G full-duplex
<i>auto</i>	Auto-negotiation.
<i>1000auto</i>	Auto-negotiation (1G full-duplex only).
<i>1000full-fiber</i>	1G full-duplex (fiber SFPs only)
<i>40000full</i>	40G full-duplex
<i>auto-module</i>	Auto Module.
<i>100FX-half</i>	100Mbps half-duplex.100Base-FX.
<i>100FX-full</i>	100Mbps full-duplex.100Base-FX.
<i>100000full</i>	100Gbps full-duplex.
<i>2500auto</i>	Auto-Negotiation (2.5Gbps Only).
<i>2500full</i>	2.5Gbps full-duplex.
<i>25000full</i>	25Gbps full-duplex.
<i>50000full</i>	50Gbps full-duplex.
<i>10000cr</i>	10Gbps copper interface.
<i>10000sr</i>	10Gbps SFI interface.
<i>100000sr4</i>	100Gbps SFI interface.
<i>100000cr4</i>	100Gbps copper interface.
<i>40000sr4</i>	40Gbps SFI interface.
<i>40000cr4</i>	40Gbps copper interface.

Parameter	Description	Type	Size	Default															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>40000auto</td><td>Auto-Negotiation (40Gbps Only).</td></tr><tr><td>25000cr</td><td>25Gbps copper interface.</td></tr><tr><td>25000sr</td><td>25Gbps SFI interface.</td></tr><tr><td>50000cr</td><td>50Gbps copper interface.</td></tr><tr><td>50000sr</td><td>50Gbps SFI interface.</td></tr><tr><td>5000auto</td><td>5Gbps full-duplex.</td></tr></table>		Option	Description	40000auto	Auto-Negotiation (40Gbps Only).	25000cr	25Gbps copper interface.	25000sr	25Gbps SFI interface.	50000cr	50Gbps copper interface.	50000sr	50Gbps SFI interface.	5000auto	5Gbps full-duplex.			
	Option	Description																	
	40000auto	Auto-Negotiation (40Gbps Only).																	
	25000cr	25Gbps copper interface.																	
	25000sr	25Gbps SFI interface.																	
	50000cr	50Gbps copper interface.																	
	50000sr	50Gbps SFI interface.																	
5000auto	5Gbps full-duplex.																		
stacking-port	Stacking port. Read-only.	integer	Minimum value: 0 0 Maximum value: 1	0															
status	Switch port admin status: up or down.	option	-	up															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>up</td><td>Set admin status up.</td></tr><tr><td>down</td><td>Set admin status down.</td></tr></table>		Option	Description	up	Set admin status up.	down	Set admin status down.											
	Option	Description																	
	up	Set admin status up.																	
down	Set admin status down.																		
sticky-mac	Enable or disable sticky-mac on the interface.	option	-	disable															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sticky mac on the interface.</td></tr><tr><td>disable</td><td>Disable sticky mac on the interface.</td></tr></table>		Option	Description	enable	Enable sticky mac on the interface.	disable	Disable sticky mac on the interface.											
	Option	Description																	
	enable	Enable sticky mac on the interface.																	
disable	Disable sticky mac on the interface.																		
storm-control-policy	Switch controller storm control policy from available options.	string	Maximum length: 63	default															
stp-bpdu-guard	Enable/disable STP BPDU guard on this interface.	option	-	disabled															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enabled</td><td>Enable STP BPDU guard on this interface.</td></tr><tr><td>disabled</td><td>Disable STP BPDU guard on this interface.</td></tr></table>		Option	Description	enabled	Enable STP BPDU guard on this interface.	disabled	Disable STP BPDU guard on this interface.											
	Option	Description																	
	enabled	Enable STP BPDU guard on this interface.																	
disabled	Disable STP BPDU guard on this interface.																		
stp-bpdu-guard-timeout	BPDU Guard disabling protection (0 - 120 min).	integer	Minimum value: 0 0 Maximum value: 120	5															
stp-root-guard	Enable/disable STP root guard on this interface.	option	-	disabled															

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enabled</i></td><td>Enable STP root-guard on this interface.</td></tr><tr><td><i>disabled</i></td><td>Disable STP root-guard on this interface.</td></tr></table>	Option	Description	<i>enabled</i>	Enable STP root-guard on this interface.	<i>disabled</i>	Disable STP root-guard on this interface.			
	Option	Description								
	<i>enabled</i>	Enable STP root-guard on this interface.								
<i>disabled</i>	Disable STP root-guard on this interface.									
stp-state	Enable/disable Spanning Tree Protocol (STP) on this interface.	option	-	enabled						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enabled</i></td><td>Enable STP on this interface.</td></tr><tr><td><i>disabled</i></td><td>Disable STP on this interface.</td></tr></table>	Option	Description	<i>enabled</i>	Enable STP on this interface.	<i>disabled</i>	Disable STP on this interface.			
	Option	Description								
	<i>enabled</i>	Enable STP on this interface.								
<i>disabled</i>	Disable STP on this interface.									
switch-id	Switch id. Read-only.	string	Maximum length: 16							
type	Interface type: physical or trunk port.	option	-	physical						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>physical</i></td><td>Physical port.</td></tr><tr><td><i>trunk</i></td><td>Trunk port.</td></tr></table>	Option	Description	<i>physical</i>	Physical port.	<i>trunk</i>	Trunk port.			
	Option	Description								
	<i>physical</i>	Physical port.								
<i>trunk</i>	Trunk port.									
untagged-vlans <vlan-name>	Configure switch port untagged VLANs. VLAN name.	string	Maximum length: 79							
vlan	Assign switch ports to a VLAN.	string	Maximum length: 15							

config dhcp-snoop-option82-override

Parameter	Description	Type	Size	Default
circuit-id	Circuit ID string.	string	Maximum length: 254	
remote-id	Remote ID string.	string	Maximum length: 254	
vlan-name	DHCP snooping option 82 VLAN.	string	Maximum length: 15	

config remote-log

Parameter	Description	Type	Size	Default
csv	Enable/disable comma-separated value (CSV) strings.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable comma-separated value (CSV) strings.		
	<i>disable</i>	Disable comma-separated value (CSV) strings.		
facility	Facility to log to remote syslog server.	option	-	local7
	Option	Description		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslogd.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	UUCP server messages.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
	<i>local3</i>	Reserved for local use.		
	<i>local4</i>	Reserved for local use.		
	<i>local5</i>	Reserved for local use.		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>local6</i>	Reserved for local use.		
	<i>local7</i>	Reserved for local use.		
name	Remote log name.	string	Maximum length: 35	
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535	514
server	IPv4 address of the remote syslog server.	string	Maximum length: 63	
severity	Severity of logs to be transferred to remote log server.	option	-	information
	Option Description			
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-	disable
	Option Description			
	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.		
	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.		

config route-offload-router

Parameter	Description	Type	Size	Default
router-ip	Router IP address.	ipv4-address	Not Specified	0.0.0.0
vlan-name	VLAN name.	string	Maximum length: 15	

config snmp-community

Parameter	Description	Type	Size	Default
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf-ip ent-conf-change l2mac
	Option	Description		
	cpu-high	Send a trap when CPU usage too high.		
	mem-low	Send a trap when available memory is low.		
	log-full	Send a trap when log disk space becomes low.		
	intf-ip	Send a trap when an interface IP address is changed.		
	ent-conf-change	Send a trap when an entity MIB change occurs (RFC4133).		
	l2mac	Send a trap for Learning event (add/delete/movefrom/moveto).		
id	SNMP community ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
name	SNMP community name.	string	Maximum length: 35	
query-v1-port	SNMP v1 query port (default = 161).	integer	Minimum value: 161 0 Maximum value: 65535	
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable SNMP v1 queries.		
	<i>enable</i>	Enable SNMP v1 queries.		
query-v2c-port	SNMP v2c query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535	161
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v2c queries.		
	<i>enable</i>	Enable SNMP v2c queries.		
status	Enable/disable this SNMP community.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP community.		
	<i>enable</i>	Enable SNMP community.		
trap-v1-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v1 traps.		
	<i>enable</i>	Enable SNMP v1 traps.		
trap-v2c-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535	162

Parameter	Description	Type	Size	Default
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v2c traps.		
	<i>enable</i>	Enable SNMP v2c traps.		

config hosts

Parameter	Description	Type	Size	Default
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

config snmp-sysinfo

Parameter	Description	Type	Size	Default
contact-info	Contact information.	string	Maximum length: 35	
description	System description.	string	Maximum length: 35	
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24	
location	System location.	string	Maximum length: 35	
status	Enable/disable SNMP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SNMP.		
	<i>enable</i>	Enable SNMP.		

config snmp-trap-threshold

Parameter	Description	Type	Size	Default
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	90
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80

config snmp-user

Parameter	Description	Type	Size	Default
auth-proto	Authentication protocol.	option	-	sha256
	Option	Description		
	md5	HMAC-MD5-96 authentication protocol.		
	sha1	HMAC-SHA-1 authentication protocol.		
	sha224	HMAC-SHA-224 authentication protocol.		
	sha256	HMAC-SHA-256 authentication protocol.		
	sha384	HMAC-SHA-384 authentication protocol.		
	sha512	HMAC-SHA-512 authentication protocol.		
auth-pwd	Password for authentication protocol.	password	Not Specified	
name	SNMP user name.	string	Maximum length: 32	
priv-proto	Privacy (encryption) protocol.	option	-	aes128
	Option	Description		
	aes128	CFB128-AES-128 symmetric encryption protocol.		
	aes192	CFB128-AES-192 symmetric encryption protocol.		
	aes192c	CFB128-AES-192-C symmetric encryption protocol.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aes256</i></td><td>CFB128-AES-256 symmetric encryption protocol.</td></tr><tr><td><i>aes256c</i></td><td>CFB128-AES-256-C symmetric encryption protocol.</td></tr><tr><td><i>des</i></td><td>CBC-DES symmetric encryption protocol.</td></tr></table>	Option	Description	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.	<i>aes256c</i>	CFB128-AES-256-C symmetric encryption protocol.	<i>des</i>	CBC-DES symmetric encryption protocol.			
	Option	Description										
	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.										
	<i>aes256c</i>	CFB128-AES-256-C symmetric encryption protocol.										
<i>des</i>	CBC-DES symmetric encryption protocol.											
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified									
queries	Enable/disable SNMP queries for this user.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SNMP queries for this user.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP queries for this user.</td></tr></table>	Option	Description	<i>disable</i>	Disable SNMP queries for this user.	<i>enable</i>	Enable SNMP queries for this user.					
	Option	Description										
	<i>disable</i>	Disable SNMP queries for this user.										
<i>enable</i>	Enable SNMP queries for this user.											
query-port	SNMPv3 query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535	161								
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-auth-no-priv</i></td><td>Message with no authentication and no privacy (encryption).</td></tr><tr><td><i>auth-no-priv</i></td><td>Message with authentication but no privacy (encryption).</td></tr><tr><td><i>auth-priv</i></td><td>Message with authentication and privacy (encryption).</td></tr></table>	Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).			
	Option	Description										
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).										
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).										
<i>auth-priv</i>	Message with authentication and privacy (encryption).											

config static-mac

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
interface	Interface name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00						
type	Type.	option	-	static						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Static MAC.</td></tr><tr><td><i>sticky</i></td><td>Sticky MAC.</td></tr></table>				Option	Description	<i>static</i>	Static MAC.	<i>sticky</i>	Sticky MAC.
	Option	Description								
	<i>static</i>	Static MAC.								
<i>sticky</i>	Sticky MAC.									
vlan	Vlan.	string	Maximum length: 15							

config storm-control

Parameter	Description	Type	Size	Default						
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Drop broadcast traffic.</td></tr><tr><td><i>disable</i></td><td>Allow broadcast traffic.</td></tr></table>	Option	Description	<i>enable</i>	Drop broadcast traffic.	<i>disable</i>	Allow broadcast traffic.			
Option	Description									
<i>enable</i>	Drop broadcast traffic.									
<i>disable</i>	Allow broadcast traffic.									
local-override	Enable to override global FortiSwitch storm control settings for this FortiSwitch.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override global storm control settings.</td></tr><tr><td><i>disable</i></td><td>Use global storm control settings.</td></tr></table>	Option	Description	<i>enable</i>	Override global storm control settings.	<i>disable</i>	Use global storm control settings.			
Option	Description									
<i>enable</i>	Override global storm control settings.									
<i>disable</i>	Use global storm control settings.									
rate	Rate in packets per second at which storm control drops excess traffic(0-10000000, default=500, drop-all=0).	integer	Minimum value: 0 Maximum value: 10000000	500						
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Drop unknown multicast traffic.</td></tr><tr><td><i>disable</i></td><td>Allow unknown multicast traffic.</td></tr></table>	Option	Description	<i>enable</i>	Drop unknown multicast traffic.	<i>disable</i>	Allow unknown multicast traffic.			
Option	Description									
<i>enable</i>	Drop unknown multicast traffic.									
<i>disable</i>	Allow unknown multicast traffic.									

Parameter	Description	Type	Size	Default
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Drop unknown unicast traffic.		
	<i>disable</i>	Allow unknown unicast traffic.		

config stp-instance

Parameter	Description	Type	Size	Default
id	Instance ID.	string	Maximum length: 2	
priority	Priority.	option	-	32768
	Option	Description		
	<i>0</i>	0.		
	<i>4096</i>	4096.		
	<i>8192</i>	8192.		
	<i>12288</i>	12288.		
	<i>16384</i>	16384.		
	<i>20480</i>	20480.		
	<i>24576</i>	24576.		
	<i>28672</i>	28672.		
	<i>32768</i>	32768.		
	<i>36864</i>	36864.		
	<i>40960</i>	40960.		
	<i>45056</i>	45056.		
	<i>49152</i>	49152.		
	<i>53248</i>	53248.		
	<i>57344</i>	57344.		
	<i>61440</i>	61440.		

config stp-settings

Parameter	Description	Type	Size	Default						
forward-time	Period of time a port is in listening and learning state (4 - 30 sec, default = 15).	integer	Minimum value: 4 Maximum value: 30	15						
hello-time	Period of time between successive STP frame Bridge Protocol Data Units (BPDUs) sent on a port (1 - 10 sec, default = 2).	integer	Minimum value: 1 Maximum value: 10	2						
local-override	Enable to configure local STP settings that override global STP settings.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override global STP settings.</td></tr><tr><td>disable</td><td>Use global STP settings.</td></tr></table>	Option	Description	enable	Override global STP settings.	disable	Use global STP settings.			
Option	Description									
enable	Override global STP settings.									
disable	Use global STP settings.									
max-age	Maximum time before a bridge port saves its configuration BPDU information (6 - 40 sec, default = 20).	integer	Minimum value: 6 Maximum value: 40	20						
max-hops	Maximum number of hops between the root bridge and the furthest bridge (1- 40, default = 20).	integer	Minimum value: 1 Maximum value: 40	20						
name	Name of local STP settings configuration.	string	Maximum length: 31							
pending-timer	Pending time (1 - 15 sec, default = 4).	integer	Minimum value: 1 Maximum value: 15	4						
revision	STP revision number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535	0						

config switch-log

Parameter	Description	Type	Size	Default																		
local-override	Enable to configure local logging settings that override global logging settings.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override global logging settings.</td></tr><tr><td>disable</td><td>Use global logging settings.</td></tr></table>	Option	Description	enable	Override global logging settings.	disable	Use global logging settings.															
Option	Description																					
enable	Override global logging settings.																					
disable	Use global logging settings.																					
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>emergency</td><td>Emergency level.</td></tr><tr><td>alert</td><td>Alert level.</td></tr><tr><td>critical</td><td>Critical level.</td></tr><tr><td>error</td><td>Error level.</td></tr><tr><td>warning</td><td>Warning level.</td></tr><tr><td>notification</td><td>Notification level.</td></tr><tr><td>information</td><td>Information level.</td></tr><tr><td>debug</td><td>Debug level.</td></tr></table>	Option	Description	emergency	Emergency level.	alert	Alert level.	critical	Critical level.	error	Error level.	warning	Warning level.	notification	Notification level.	information	Information level.	debug	Debug level.			
Option	Description																					
emergency	Emergency level.																					
alert	Alert level.																					
critical	Critical level.																					
error	Error level.																					
warning	Warning level.																					
notification	Notification level.																					
information	Information level.																					
debug	Debug level.																					
status	Enable/disable adding FortiSwitch logs to the FortiGate event log.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Add FortiSwitch logs to the FortiGate event log.</td></tr><tr><td>disable</td><td>Do not add FortiSwitch logs to the FortiGate event log.</td></tr></table>	Option	Description	enable	Add FortiSwitch logs to the FortiGate event log.	disable	Do not add FortiSwitch logs to the FortiGate event log.															
Option	Description																					
enable	Add FortiSwitch logs to the FortiGate event log.																					
disable	Do not add FortiSwitch logs to the FortiGate event log.																					

config vlan

Parameter	Description	Type	Size	Default
assignment-priority	802.1x Radius (Tunnel-Private-Group-Id) VLANID assign-by-name priority. A smaller value has a higher priority.	integer	Minimum value: 1 Maximum value: 255	128
vlan-name	VLAN name.	string	Maximum length: 15	

config switch-controller network-monitor-settings



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure network monitor settings.

```
config switch-controller network-monitor-settings
    Description: Configure network monitor settings.
    set network-monitoring [enable|disable]
end
```

config switch-controller network-monitor-settings

Parameter	Description	Type	Size	Default						
network-monitoring	Enable/disable passive gathering of information by FortiSwitch units concerning other network devices.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable network monitoring on FortiSwitch.</td></tr><tr><td><i>disable</i></td><td>Disable network monitoring on FortiSwitch.</td></tr></table>	Option	Description	<i>enable</i>	Enable network monitoring on FortiSwitch.	<i>disable</i>	Disable network monitoring on FortiSwitch.			
Option	Description									
<i>enable</i>	Enable network monitoring on FortiSwitch.									
<i>disable</i>	Disable network monitoring on FortiSwitch.									

config switch-controller ptp interface-policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

PTP interface-policy configuration.

```
config switch-controller ptp interface-policy
  Description: PTP interface-policy configuration.
  edit <name>
    set description {string}
    set vlan {string}
    set vlan-pri {integer}
  next
end
```

config switch-controller ptp interface-policy

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
name	Policy name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
vlan	PTP VLAN.	string	Maximum length: 15	
vlan-pri	Configure PTP VLAN priority (0 - 7, default = 4).	integer	Minimum value: 0 Maximum value: 7	4

config switch-controller ptp profile



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Global PTP profile.

```
config switch-controller ptp profile
  Description: Global PTP profile.
  edit <name>
    set description {string}
    set domain {integer}
    set mode [transparent-e2e|transparent-p2p]
    set pdelay-req-interval [1sec|2sec|...]
    set ptp-profile {option}
    set transport {option}
  next
end
```

config switch-controller ptp profile

Parameter	Description	Type	Size	Default														
description	Description.	string	Maximum length: 63															
domain	Configure PTP domain value (0 - 255, default = 254).	integer	Minimum value: 0 Maximum value: 255	254														
mode	Select PTP mode.	option	-	transparent-e2e														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>transparent-e2e</i></td><td>End-to-end transparent clock.</td></tr><tr><td><i>transparent-p2p</i></td><td>Peer-to-peer transparent clock.</td></tr></table>				Option	Description	<i>transparent-e2e</i>	End-to-end transparent clock.	<i>transparent-p2p</i>	Peer-to-peer transparent clock.								
Option	Description																	
<i>transparent-e2e</i>	End-to-end transparent clock.																	
<i>transparent-p2p</i>	Peer-to-peer transparent clock.																	
name	Profile name.	string	Maximum length: 63															
pdelay-req-interval	Configure PTP peer delay request interval.	option	-	1sec														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1sec</i></td><td>1 sec.</td></tr><tr><td><i>2sec</i></td><td>2 sec.</td></tr><tr><td><i>4sec</i></td><td>4 sec.</td></tr><tr><td><i>8sec</i></td><td>8 sec.</td></tr><tr><td><i>16sec</i></td><td>16 sec.</td></tr><tr><td><i>32sec</i></td><td>32 sec.</td></tr></table>				Option	Description	<i>1sec</i>	1 sec.	<i>2sec</i>	2 sec.	<i>4sec</i>	4 sec.	<i>8sec</i>	8 sec.	<i>16sec</i>	16 sec.	<i>32sec</i>	32 sec.
Option	Description																	
<i>1sec</i>	1 sec.																	
<i>2sec</i>	2 sec.																	
<i>4sec</i>	4 sec.																	
<i>8sec</i>	8 sec.																	
<i>16sec</i>	16 sec.																	
<i>32sec</i>	32 sec.																	
ptp-profile	Configure PTP power profile.	option	-	C37.238-2017														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>C37.238-2017</i></td><td>C37.238-2017 power profile.</td></tr></table>				Option	Description	<i>C37.238-2017</i>	C37.238-2017 power profile.										
Option	Description																	
<i>C37.238-2017</i>	C37.238-2017 power profile.																	
transport	Configure PTP transport mode.	option	-	I2-mcast														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>I2-mcast</i></td><td>L2 multicast.</td></tr></table>				Option	Description	<i>I2-mcast</i>	L2 multicast.										
Option	Description																	
<i>I2-mcast</i>	L2 multicast.																	

config switch-controller qos dot1p-map



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS 802.1p.

```
config switch-controller qos dot1p-map
  Description: Configure FortiSwitch QoS 802.1p.
  edit <name>
    set description {string}
    set egress-pri-tagging [disable|enable]
    set priority-0 [queue-0|queue-1|...]
    set priority-1 [queue-0|queue-1|...]
    set priority-2 [queue-0|queue-1|...]
    set priority-3 [queue-0|queue-1|...]
    set priority-4 [queue-0|queue-1|...]
    set priority-5 [queue-0|queue-1|...]
    set priority-6 [queue-0|queue-1|...]
    set priority-7 [queue-0|queue-1|...]
  next
end
```

config switch-controller qos dot1p-map

Parameter	Description	Type	Size	Default
description	Description of the 802.1p name.	string	Maximum length: 63	
egress-pri-tagging	Enable/disable egress priority-tag frame.	option	-	disable
	Option	Description		
	disable	Disable egress priority tagging.		
	enable	Enable egress priority tagging.		
name	Dot1p map name.	string	Maximum length: 63	
priority-0	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	queue-0	COS queue 0 (lowest priority).		
	queue-1	COS queue 1.		
	queue-2	COS queue 2.		
	queue-3	COS queue 3.		
	queue-4	COS queue 4.		
	queue-5	COS queue 5.		
	queue-6	COS queue 6.		
	queue-7	COS queue 7 (highest priority).		
priority-1	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	queue-0	COS queue 0 (lowest priority).		
	queue-1	COS queue 1.		
	queue-2	COS queue 2.		
	queue-3	COS queue 3.		
	queue-4	COS queue 4.		
	queue-5	COS queue 5.		
	queue-6	COS queue 6.		
	queue-7	COS queue 7 (highest priority).		

Parameter	Description	Type	Size	Default
priority-2	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-3	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-4	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-5	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-6	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-7	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		

config switch-controller qos ip-dscp-map



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS IP precedence/DSCP.

```
config switch-controller qos ip-dscp-map
  Description: Configure FortiSwitch QoS IP precedence/DSCP.
  edit <name>
    set description {string}
    config map
      Description: Maps between IP-DSCP value to COS queue.
      edit <name>
        set cos-queue {integer}
        set diffserv {option1}, {option2}, ...
        set ip-precedence {option1}, {option2}, ...
```

```

        set value {user}
    next
end
next
end

```

config switch-controller qos ip-dscp-map

Parameter	Description	Type	Size	Default
description	Description of the ip-dscp map name.	string	Maximum length: 63	
name	Dscp map name.	string	Maximum length: 63	

config map

Parameter	Description	Type	Size	Default
cos-queue	COS queue number.	integer	Minimum value: 0 Maximum value: 7	0
diffserv	Differentiated service.	option	-	
	Option	Description		
	CS0	DSCP CS0.		
	CS1	DSCP CS1.		
	AF11	DSCP AF11.		
	AF12	DSCP AF12.		
	AF13	DSCP AF13.		
	CS2	DSCP CS2.		
	AF21	DSCP AF21.		
	AF22	DSCP AF22.		
	AF23	DSCP AF23.		
	CS3	DSCP CS3.		
	AF31	DSCP AF31.		
	AF32	DSCP AF32.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>AF33</td><td>DSCP AF33.</td></tr><tr><td>CS4</td><td>DSCP CS4.</td></tr><tr><td>AF41</td><td>DSCP AF41.</td></tr><tr><td>AF42</td><td>DSCP AF42.</td></tr><tr><td>AF43</td><td>DSCP AF43.</td></tr><tr><td>CS5</td><td>DSCP CS5.</td></tr><tr><td>EF</td><td>DSCP EF.</td></tr><tr><td>CS6</td><td>DSCP CS6.</td></tr><tr><td>CS7</td><td>DSCP CS7.</td></tr></table>	Option	Description	AF33	DSCP AF33.	CS4	DSCP CS4.	AF41	DSCP AF41.	AF42	DSCP AF42.	AF43	DSCP AF43.	CS5	DSCP CS5.	EF	DSCP EF.	CS6	DSCP CS6.	CS7	DSCP CS7.			
	Option	Description																						
	AF33	DSCP AF33.																						
	CS4	DSCP CS4.																						
	AF41	DSCP AF41.																						
	AF42	DSCP AF42.																						
	AF43	DSCP AF43.																						
	CS5	DSCP CS5.																						
	EF	DSCP EF.																						
	CS6	DSCP CS6.																						
CS7	DSCP CS7.																							
ip-precedence	IP Precedence.	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>network-control</td><td>Network control.</td></tr><tr><td>internetwork-control</td><td>Internetwork control.</td></tr><tr><td>critic-ecp</td><td>Critic ECP.</td></tr><tr><td>flashoverride</td><td>Flash override.</td></tr><tr><td>flash</td><td>Flash.</td></tr><tr><td>immediate</td><td>Immediate.</td></tr><tr><td>priority</td><td>Priority.</td></tr><tr><td>routine</td><td>Routine.</td></tr></table>	Option	Description	network-control	Network control.	internetwork-control	Internetwork control.	critic-ecp	Critic ECP.	flashoverride	Flash override.	flash	Flash.	immediate	Immediate.	priority	Priority.	routine	Routine.					
	Option	Description																						
	network-control	Network control.																						
	internetwork-control	Internetwork control.																						
	critic-ecp	Critic ECP.																						
	flashoverride	Flash override.																						
	flash	Flash.																						
	immediate	Immediate.																						
	priority	Priority.																						
routine	Routine.																							
name	Dscp mapping entry name.	string	Maximum length: 63																					
value	Raw values of DSCP (0 - 63).	user	Not Specified																					

config switch-controller qos qos-policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS policy.

```
config switch-controller qos qos-policy
  Description: Configure FortiSwitch QoS policy.
  edit <name>
    set default-cos {integer}
    set queue-policy {string}
    set trust-dot1p-map {string}
    set trust-ip-dscp-map {string}
  next
end
```

config switch-controller qos qos-policy

Parameter	Description	Type	Size	Default
default-cos	Default cos queue for untagged packets.	integer	Minimum value: 0 Maximum value: 7	0

Parameter	Description	Type	Size	Default
name	QoS policy name.	string	Maximum length: 63	
queue-policy	QoS egress queue policy.	string	Maximum length: 63	default
trust-dot1p-map	QoS trust 802.1p map.	string	Maximum length: 63	
trust-ip-dscp-map	QoS trust ip dscp map.	string	Maximum length: 63	

config switch-controller qos queue-policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS egress queue policy.

```
config switch-controller qos queue-policy
  Description: Configure FortiSwitch QoS egress queue policy.
  edit <name>
    config cos-queue
      Description: COS queue configuration.
      edit <name>
        set description {string}
        set drop-policy [taildrop|weighted-random-early-detection]
```

```

        set ecn [disable|enable]
        set max-rate {integer}
        set max-rate-percent {integer}
        set min-rate {integer}
        set min-rate-percent {integer}
        set weight {integer}
    next
end
set rate-by [kbps|percent]
set schedule [strict|round-robin|...]
next
end

```

config switch-controller qos queue-policy

Parameter	Description	Type	Size	Default								
name	QoS policy name.	string	Maximum length: 63									
rate-by	COS queue rate by kbps or percent.	option	-	kbps								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kbps</i></td><td>Rate by kbps.</td></tr><tr><td><i>percent</i></td><td>Rate by percent.</td></tr></table>	Option	Description	<i>kbps</i>	Rate by kbps.	<i>percent</i>	Rate by percent.					
Option	Description											
<i>kbps</i>	Rate by kbps.											
<i>percent</i>	Rate by percent.											
schedule	COS queue scheduling.	option	-	round-robin								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>strict</i></td><td>Strict scheduling (queue7: highest priority, queue0: lowest priority).</td></tr><tr><td><i>round-robin</i></td><td>Round robin scheduling.</td></tr><tr><td><i>weighted</i></td><td>Weighted round robin scheduling.</td></tr></table>	Option	Description	<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).	<i>round-robin</i>	Round robin scheduling.	<i>weighted</i>	Weighted round robin scheduling.			
Option	Description											
<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).											
<i>round-robin</i>	Round robin scheduling.											
<i>weighted</i>	Weighted round robin scheduling.											

config cos-queue

Parameter	Description	Type	Size	Default				
description	Description of the COS queue.	string	Maximum length: 63					
drop-policy	COS queue drop policy.	option	-	taildrop				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>taildrop</i></td><td>Taildrop policy.</td></tr></table>				Option	Description	<i>taildrop</i>	Taildrop policy.
Option	Description							
<i>taildrop</i>	Taildrop policy.							

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weighted-random-early-detection</i></td><td>Weighted random early detection drop policy.</td></tr></table>	Option	Description	<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.					
	Option	Description								
	<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.								
ecn	Enable/disable ECN packet marking to drop eligible packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable ECN packet marking to drop eligible packets.</td></tr><tr><td><i>enable</i></td><td>Enable ECN packet marking to drop eligible packets.</td></tr></table>	Option	Description	<i>disable</i>	Disable ECN packet marking to drop eligible packets.	<i>enable</i>	Enable ECN packet marking to drop eligible packets.			
	Option	Description								
	<i>disable</i>	Disable ECN packet marking to drop eligible packets.								
<i>enable</i>	Enable ECN packet marking to drop eligible packets.									
max-rate	Maximum rate (0 - 4294967295 kbps, 0 to disable).	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-rate-percent	Maximum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295	0						
min-rate	Minimum rate (0 - 4294967295 kbps, 0 to disable).	integer	Minimum value: 0 Maximum value: 4294967295	0						
min-rate-percent	Minimum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295	0						
name	Cos queue ID.	string	Maximum length: 63							
weight	Weight of weighted round robin scheduling.	integer	Minimum value: 1 Maximum value: 4294967295	1						

config switch-controller quarantine



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch quarantine support.

```
config switch-controller quarantine
  Description: Configure FortiSwitch quarantine support.
  set quarantine [enable|disable]
  config targets
    Description: Quarantine MACs.
    edit <mac>
      set description {string}
      set tag <tags1>, <tags2>, ...
    next
  end
end
```

config switch-controller quarantine

Parameter	Description	Type	Size	Default
quarantine	Enable/disable quarantine.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable quarantine.		
	<i>disable</i>	Disable quarantine.		

config targets

Parameter	Description	Type	Size	Default
description	Description for the quarantine MAC.	string	Maximum length: 63	
mac	Quarantine MAC.	mac-address	Not Specified	00:00:00:00:00:00
tag <tags>	Tags for the quarantine MAC. Tag string. For example, string1 string2 string3.	string	Maximum length: 63	

config switch-controller remote-log



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure logging by FortiSwitch device to a remote syslog server.

```

config switch-controller remote-log
    Description: Configure logging by FortiSwitch device to a remote syslog server.
    edit <name>
        set csv [enable|disable]
        set facility [kernel|user|...]
        set port {integer}
        set server {string}
        set severity [emergency|alert|...]
        set status [enable|disable]
    next
end

```

config switch-controller remote-log

Parameter	Description	Type	Size	Default
csv	Enable/disable comma-separated value (CSV) strings.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable comma-separated value (CSV) strings.		
	<i>disable</i>	Disable comma-separated value (CSV) strings.		
facility	Facility to log to remote syslog server.	option	-	local7
	Option	Description		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslogd.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	UUCP server messages.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																										
	<i>audit</i>	Log audit.																										
	<i>alert</i>	Log alert.																										
	<i>clock</i>	Clock daemon.																										
	<i>local0</i>	Reserved for local use.																										
	<i>local1</i>	Reserved for local use.																										
	<i>local2</i>	Reserved for local use.																										
	<i>local3</i>	Reserved for local use.																										
	<i>local4</i>	Reserved for local use.																										
	<i>local5</i>	Reserved for local use.																										
	<i>local6</i>	Reserved for local use.																										
<i>local7</i>	Reserved for local use.																											
name	Remote log name.	string	Maximum length: 35																									
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535	514																								
server	IPv4 address of the remote syslog server.	string	Maximum length: 63																									
severity	Severity of logs to be transferred to remote log server.	option	-	information																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.									
	Option	Description																										
	<i>emergency</i>	Emergency level.																										
	<i>alert</i>	Alert level.																										
	<i>critical</i>	Critical level.																										
	<i>error</i>	Error level.																										
	<i>warning</i>	Warning level.																										
	<i>notification</i>	Notification level.																										
<i>information</i>	Information level.																											
<i>debug</i>	Debug level.																											

Parameter	Description	Type	Size	Default
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-	disable
Option	Description			
<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.			
<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.			

config switch-controller security-policy 802-1X



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure 802.1x MAC Authentication Bypass (MAB) policies.

```
config switch-controller security-policy 802-1X
  Description: Configure 802.1x MAC Authentication Bypass (MAB) policies.
  edit <name>
    set auth-fail-vlan [disable|enable]
    set auth-fail-vlan-id {string}
    set auth-order [dot1x-mab|mab-dot1x|...]
    set auth-priority [legacy|dot1x-mab|...]
    set authserver-timeout-period {integer}
    set authserver-timeout-tagged [disable|lldp-voice|...]
    set authserver-timeout-tagged-vlanid {string}
```

```

set authserver-timeout-vlan [disable|enable]
set authserver-timeout-vlanid {string}
set dacl [disable|enable]
set eap-auto-untagged-vlans [disable|enable]
set eap-passthru [disable|enable]
set framevid-apply [disable|enable]
set guest-auth-delay {integer}
set guest-vlan [disable|enable]
set guest-vlan-id {string}
set mac-auth-bypass [disable|enable]
set open-auth [disable|enable]
set policy-type {option}
set radius-timeout-overwrite [disable|enable]
set security-mode [802.1X|802.1X-mac-based]
set user-group <name1>, <name2>, ...
next
end

```

config switch-controller security-policy 802-1X

Parameter	Description	Type	Size	Default								
auth-fail-vlan	Enable to allow limited access to clients that cannot authenticate.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable authentication fail VLAN on this interface.</td></tr><tr><td>enable</td><td>Enable authentication fail VLAN on this interface.</td></tr></table>	Option	Description	disable	Disable authentication fail VLAN on this interface.	enable	Enable authentication fail VLAN on this interface.					
Option	Description											
disable	Disable authentication fail VLAN on this interface.											
enable	Enable authentication fail VLAN on this interface.											
auth-fail-vlan-id	VLAN ID on which authentication failed.	string	Maximum length: 15									
auth-order	Configure authentication order.	option	-	mab-dot1x								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dot1x-mab</td><td>Use EAP 1X authentication first then MAB.</td></tr><tr><td>mab-dot1x</td><td>Use MAB authentication first then EAP 1X.</td></tr><tr><td>mab</td><td>Use MAB authentication only.</td></tr></table>	Option	Description	dot1x-mab	Use EAP 1X authentication first then MAB.	mab-dot1x	Use MAB authentication first then EAP 1X.	mab	Use MAB authentication only.			
Option	Description											
dot1x-mab	Use EAP 1X authentication first then MAB.											
mab-dot1x	Use MAB authentication first then EAP 1X.											
mab	Use MAB authentication only.											
auth-priority	Configure authentication priority.	option	-	legacy								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>legacy</td><td>EAP 1X authentication has a higher priority than MAB with the legacy implementation.</td></tr><tr><td>dot1x-mab</td><td>EAP 1X authentication has a higher priority than MAB.</td></tr></table>	Option	Description	legacy	EAP 1X authentication has a higher priority than MAB with the legacy implementation.	dot1x-mab	EAP 1X authentication has a higher priority than MAB.					
Option	Description											
legacy	EAP 1X authentication has a higher priority than MAB with the legacy implementation.											
dot1x-mab	EAP 1X authentication has a higher priority than MAB.											

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mab-dot1x</i></td><td>MAB authentication has a higher priority than EAP 1X.</td></tr></table>	Option	Description	<i>mab-dot1x</i>	MAB authentication has a higher priority than EAP 1X.							
Option	Description											
<i>mab-dot1x</i>	MAB authentication has a higher priority than EAP 1X.											
authserver-timeout-period	Authentication server timeout period (3 - 15 sec, default = 3).	integer	Minimum value: 3 Maximum value: 15	3								
authserver-timeout-tagged	Configure timeout option for the tagged VLAN which allows limited access when the authentication server is unavailable.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication server timeout on this interface.</td></tr><tr><td><i>lldp-voice</i></td><td>LLDP voice timeout for the tagged VLAN on this interface.</td></tr><tr><td><i>static</i></td><td>Static timeout for the tagged VLAN on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable authentication server timeout on this interface.	<i>lldp-voice</i>	LLDP voice timeout for the tagged VLAN on this interface.	<i>static</i>	Static timeout for the tagged VLAN on this interface.			
Option	Description											
<i>disable</i>	Disable authentication server timeout on this interface.											
<i>lldp-voice</i>	LLDP voice timeout for the tagged VLAN on this interface.											
<i>static</i>	Static timeout for the tagged VLAN on this interface.											
authserver-timeout-tagged-vlanid	Tagged VLAN name for which the timeout option is applied to (only one VLAN ID).	string	Maximum length: 15									
authserver-timeout-vlan	Enable/disable the authentication server timeout VLAN to allow limited access when RADIUS is unavailable.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication server timeout VLAN on this interface.</td></tr><tr><td><i>enable</i></td><td>Enable authentication server timeout VLAN on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable authentication server timeout VLAN on this interface.	<i>enable</i>	Enable authentication server timeout VLAN on this interface.					
Option	Description											
<i>disable</i>	Disable authentication server timeout VLAN on this interface.											
<i>enable</i>	Enable authentication server timeout VLAN on this interface.											
authserver-timeout-vlanid	Authentication server timeout VLAN name.	string	Maximum length: 15									
dacl	Enable/disable dynamic access control list on this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dynamic access control list on this interface.</td></tr><tr><td><i>enable</i></td><td>Enable dynamic access control on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable dynamic access control list on this interface.	<i>enable</i>	Enable dynamic access control on this interface.					
Option	Description											
<i>disable</i>	Disable dynamic access control list on this interface.											
<i>enable</i>	Enable dynamic access control on this interface.											
eap-auto-untagged-vlans	Enable/disable automatic inclusion of untagged VLANs.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable automatic inclusion of untagged VLANs.		
	<i>enable</i>	Enable automatic inclusion of untagged VLANs.		
eap-passthru	Enable/disable EAP pass-through mode, allowing protocols (such as LLDP) to pass through ports for more flexible authentication.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable EAP pass-through mode on this interface.		
	<i>enable</i>	Enable EAP pass-through mode on this interface.		
framevid-apply	Enable/disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.		
	<i>enable</i>	Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.		
guest-auth-delay	Guest authentication delay (1 - 900 sec, default = 30).	integer	Minimum value: 1 Maximum value: 900	30
guest-vlan	Enable the guest VLAN feature to allow limited access to non-802.1X-compliant clients.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable guest VLAN on this interface.		
	<i>enable</i>	Enable guest VLAN on this interface.		
guest-vlan-id	Guest VLAN name.	string	Maximum length: 15	
mac-auth-bypass	Enable/disable MAB for this policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable MAB.		
	<i>enable</i>	Enable MAB.		

Parameter	Description	Type	Size	Default						
name	Policy name.	string	Maximum length: 31							
open-auth	Enable/disable open authentication for this policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable open authentication.</td></tr><tr><td><i>enable</i></td><td>Enable open authentication.</td></tr></table>	Option	Description	<i>disable</i>	Disable open authentication.	<i>enable</i>	Enable open authentication.			
Option	Description									
<i>disable</i>	Disable open authentication.									
<i>enable</i>	Enable open authentication.									
policy-type	Policy type.	option	-	802.1X						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.1X</i></td><td>802.1X security policy.</td></tr></table>	Option	Description	<i>802.1X</i>	802.1X security policy.					
Option	Description									
<i>802.1X</i>	802.1X security policy.									
radius-timeout-overwrite	Enable to override the global RADIUS session timeout.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Override the global RADIUS session timeout.</td></tr><tr><td><i>enable</i></td><td>Use the global RADIUS session timeout.</td></tr></table>	Option	Description	<i>disable</i>	Override the global RADIUS session timeout.	<i>enable</i>	Use the global RADIUS session timeout.			
Option	Description									
<i>disable</i>	Override the global RADIUS session timeout.									
<i>enable</i>	Use the global RADIUS session timeout.									
security-mode	Port or MAC based 802.1X security mode.	option	-	802.1X						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.1X</i></td><td>802.1X port based authentication.</td></tr><tr><td><i>802.1X-mac-based</i></td><td>802.1X MAC based authentication.</td></tr></table>	Option	Description	<i>802.1X</i>	802.1X port based authentication.	<i>802.1X-mac-based</i>	802.1X MAC based authentication.			
Option	Description									
<i>802.1X</i>	802.1X port based authentication.									
<i>802.1X-mac-based</i>	802.1X MAC based authentication.									
user-group <name>	Name of user-group to assign to this MAC Authentication Bypass (MAB) policy. Group name.	string	Maximum length: 79							

config switch-controller security-policy local-access



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure allowaccess list for mgmt and internal interfaces on managed FortiSwitch units.

```
config switch-controller security-policy local-access
    Description: Configure allowaccess list for mgmt and internal interfaces on managed
FortiSwitch units.
    edit <name>
        set internal-allowaccess {option1}, {option2}, ...
        set mgmt-allowaccess {option1}, {option2}, ...
    next
end
```

config switch-controller security-policy local-access

Parameter	Description	Type	Size	Default
internal-allowaccess	Allowed access on the switch internal interface.	option	-	https ping ssh
	Option	Description		
	https	HTTPS access.		

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>radius-acct</i></td><td>RADIUS accounting access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>radius-acct</i>	RADIUS accounting access.					
	Option	Description																		
	<i>ping</i>	PING access.																		
	<i>ssh</i>	SSH access.																		
	<i>snmp</i>	SNMP access.																		
	<i>http</i>	HTTP access.																		
	<i>telnet</i>	TELNET access.																		
<i>radius-acct</i>	RADIUS accounting access.																			
mgmt-allowaccess	Allowed access on the switch management interface.	option	-	https ping ssh																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>radius-acct</i></td><td>RADIUS accounting access.</td></tr></table>	Option	Description	<i>https</i>	HTTPS access.	<i>ping</i>	PING access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>radius-acct</i>	RADIUS accounting access.			
	Option	Description																		
	<i>https</i>	HTTPS access.																		
	<i>ping</i>	PING access.																		
	<i>ssh</i>	SSH access.																		
	<i>snmp</i>	SNMP access.																		
	<i>http</i>	HTTP access.																		
<i>telnet</i>	TELNET access.																			
<i>radius-acct</i>	RADIUS accounting access.																			
name	Policy name.	string	Maximum length: 31																	

config switch-controller sflow



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch sFlow.

```
config switch-controller sflow
    Description: Configure FortiSwitch sFlow.
    set collector-ip {ipv4-address}
    set collector-port {integer}
end
```

config switch-controller sflow

Parameter	Description	Type	Size	Default
collector-ip	Collector IP.	ipv4-address	Not Specified	0.0.0.0
collector-port	SFlow collector port (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535	6343

config switch-controller snmp-community



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP v1/v2c communities globally.

```
config switch-controller snmp-community
  Description: Configure FortiSwitch SNMP v1/v2c communities globally.
  edit <id>
    set events {option1}, {option2}, ...
    config hosts
      Description: Configure IPv4 SNMP managers (hosts).
      edit <id>
        set ip {user}
      next
    end
    set name {string}
    set query-v1-port {integer}
    set query-v1-status [disable|enable]
    set query-v2c-port {integer}
    set query-v2c-status [disable|enable]
    set status [disable|enable]
    set trap-v1-lport {integer}
    set trap-v1-rport {integer}
    set trap-v1-status [disable|enable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set trap-v2c-status [disable|enable]
```

```
next
end
```

config switch-controller snmp-community

Parameter	Description	Type	Size	Default														
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf- ip ent-conf- change l2mac														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cpu-high</td><td>Send a trap when CPU usage too high.</td></tr><tr><td>mem-low</td><td>Send a trap when available memory is low.</td></tr><tr><td>log-full</td><td>Send a trap when log disk space becomes low.</td></tr><tr><td>intf-ip</td><td>Send a trap when an interface IP address is changed.</td></tr><tr><td>ent-conf-change</td><td>Send a trap when an entity MIB change occurs (RFC4133).</td></tr><tr><td>l2mac</td><td>Send a trap for Learning event (add/delete/movefrom/moveto).</td></tr></table>	Option	Description	cpu-high	Send a trap when CPU usage too high.	mem-low	Send a trap when available memory is low.	log-full	Send a trap when log disk space becomes low.	intf-ip	Send a trap when an interface IP address is changed.	ent-conf-change	Send a trap when an entity MIB change occurs (RFC4133).	l2mac	Send a trap for Learning event (add/delete/movefrom/moveto).			
Option	Description																	
cpu-high	Send a trap when CPU usage too high.																	
mem-low	Send a trap when available memory is low.																	
log-full	Send a trap when log disk space becomes low.																	
intf-ip	Send a trap when an interface IP address is changed.																	
ent-conf-change	Send a trap when an entity MIB change occurs (RFC4133).																	
l2mac	Send a trap for Learning event (add/delete/movefrom/moveto).																	
id	SNMP community ID.	integer	Minimum value: 0 0 Maximum value: 4294967295															
name	SNMP community name.	string	Maximum length: 35															
query-v1-port	SNMP v1 query port (default = 161).	integer	Minimum value: 161 0 Maximum value: 65535															
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SNMP v1 queries.</td></tr><tr><td>enable</td><td>Enable SNMP v1 queries.</td></tr></table>	Option	Description	disable	Disable SNMP v1 queries.	enable	Enable SNMP v1 queries.											
Option	Description																	
disable	Disable SNMP v1 queries.																	
enable	Enable SNMP v1 queries.																	
query-v2c-port	SNMP v2c query port (default = 161).	integer	Minimum value: 161 0 Maximum value: 65535															

Parameter	Description	Type	Size	Default
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v2c queries.		
	<i>enable</i>	Enable SNMP v2c queries.		
status	Enable/disable this SNMP community.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP community.		
	<i>enable</i>	Enable SNMP community.		
trap-v1-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v1 traps.		
	<i>enable</i>	Enable SNMP v1 traps.		
trap-v2c-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v2c traps.		
	<i>enable</i>	Enable SNMP v2c traps.		

config hosts

Parameter	Description	Type	Size	Default
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

config switch-controller snmp-sysinfo



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R. It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP system information globally.

```
config switch-controller snmp-sysinfo
  Description: Configure FortiSwitch SNMP system information globally.
  set contact-info {string}
  set description {string}
  set engine-id {string}
  set location {string}
  set status [disable|enable]
end
```


config switch-controller snmp-sysinfo

Parameter	Description	Type	Size	Default
contact-info	Contact information.	string	Maximum length: 35	
description	System description.	string	Maximum length: 35	
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24	
location	System location.	string	Maximum length: 35	
status	Enable/disable SNMP.	option	-	disable
		Option	Description	
		disable	Disable SNMP.	
		enable	Enable SNMP.	

config switch-controller snmp-trap-threshold



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP trap threshold values globally.

```
config switch-controller snmp-trap-threshold
  Description: Configure FortiSwitch SNMP trap threshold values globally.
  set trap-high-cpu-threshold {integer}
  set trap-log-full-threshold {integer}
  set trap-low-memory-threshold {integer}
end
```

config switch-controller snmp-trap-threshold

Parameter	Description	Type	Size	Default
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	90
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80

config switch-controller snmp-user



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP v3 users globally.

```
config switch-controller snmp-user
  Description: Configure FortiSwitch SNMP v3 users globally.
  edit <name>
    set auth-proto [md5|sha1|...]
    set auth-pwd {password}
    set priv-proto [aes128|aes192|...]
    set priv-pwd {password}
    set queries [disable|enable]
    set query-port {integer}
    set security-level [no-auth-no-priv|auth-no-priv|...]
  next
end
```

config switch-controller snmp-user

Parameter	Description	Type	Size	Default
auth-proto	Authentication protocol.	option	-	sha256

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>md5</td><td>HMAC-MD5-96 authentication protocol.</td></tr><tr><td>sha1</td><td>HMAC-SHA-1 authentication protocol.</td></tr><tr><td>sha224</td><td>HMAC-SHA-224 authentication protocol.</td></tr><tr><td>sha256</td><td>HMAC-SHA-256 authentication protocol.</td></tr><tr><td>sha384</td><td>HMAC-SHA-384 authentication protocol.</td></tr><tr><td>sha512</td><td>HMAC-SHA-512 authentication protocol.</td></tr></table>	Option	Description	md5	HMAC-MD5-96 authentication protocol.	sha1	HMAC-SHA-1 authentication protocol.	sha224	HMAC-SHA-224 authentication protocol.	sha256	HMAC-SHA-256 authentication protocol.	sha384	HMAC-SHA-384 authentication protocol.	sha512	HMAC-SHA-512 authentication protocol.			
	Option	Description																
	md5	HMAC-MD5-96 authentication protocol.																
	sha1	HMAC-SHA-1 authentication protocol.																
	sha224	HMAC-SHA-224 authentication protocol.																
	sha256	HMAC-SHA-256 authentication protocol.																
	sha384	HMAC-SHA-384 authentication protocol.																
	sha512	HMAC-SHA-512 authentication protocol.																
auth-pwd	Password for authentication protocol.	password	Not Specified															
name	SNMP user name.	string	Maximum length: 32															
priv-proto	Privacy (encryption) protocol.	option	-	aes128														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>aes128</td><td>CFB128-AES-128 symmetric encryption protocol.</td></tr><tr><td>aes192</td><td>CFB128-AES-192 symmetric encryption protocol.</td></tr><tr><td>aes192c</td><td>CFB128-AES-192-C symmetric encryption protocol.</td></tr><tr><td>aes256</td><td>CFB128-AES-256 symmetric encryption protocol.</td></tr><tr><td>aes256c</td><td>CFB128-AES-256-C symmetric encryption protocol.</td></tr><tr><td>des</td><td>CBC-DES symmetric encryption protocol.</td></tr></table>	Option	Description	aes128	CFB128-AES-128 symmetric encryption protocol.	aes192	CFB128-AES-192 symmetric encryption protocol.	aes192c	CFB128-AES-192-C symmetric encryption protocol.	aes256	CFB128-AES-256 symmetric encryption protocol.	aes256c	CFB128-AES-256-C symmetric encryption protocol.	des	CBC-DES symmetric encryption protocol.			
	Option	Description																
	aes128	CFB128-AES-128 symmetric encryption protocol.																
	aes192	CFB128-AES-192 symmetric encryption protocol.																
	aes192c	CFB128-AES-192-C symmetric encryption protocol.																
	aes256	CFB128-AES-256 symmetric encryption protocol.																
	aes256c	CFB128-AES-256-C symmetric encryption protocol.																
	des	CBC-DES symmetric encryption protocol.																
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified															
queries	Enable/disable SNMP queries for this user.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SNMP queries for this user.</td></tr><tr><td>enable</td><td>Enable SNMP queries for this user.</td></tr></table>	Option	Description	disable	Disable SNMP queries for this user.	enable	Enable SNMP queries for this user.											
	Option	Description																
	disable	Disable SNMP queries for this user.																
enable	Enable SNMP queries for this user.																	
query-port	SNMPv3 query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535	161														
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).		
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).		
	<i>auth-priv</i>	Message with authentication and privacy (encryption).		

config switch-controller storm-control



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch storm control.

```
config switch-controller storm-control
    Description: Configure FortiSwitch storm control.
    set broadcast [enable|disable]
    set rate {integer}
    set unknown-multicast [enable|disable]
    set unknown-unicast [enable|disable]
end
```

config switch-controller storm-control

Parameter	Description	Type	Size	Default						
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcast storm control.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast storm control.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcast storm control.	<i>disable</i>	Disable broadcast storm control.			
Option	Description									
<i>enable</i>	Enable broadcast storm control.									
<i>disable</i>	Disable broadcast storm control.									
rate	Rate in packets per second at which storm control drops excess traffic(0-10000000, default=500, drop-all=0).	integer	Minimum value: 0 Maximum value: 10000000	500						
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unknown multicast storm control.</td></tr><tr><td><i>disable</i></td><td>Disable unknown multicast storm control.</td></tr></table>	Option	Description	<i>enable</i>	Enable unknown multicast storm control.	<i>disable</i>	Disable unknown multicast storm control.			
Option	Description									
<i>enable</i>	Enable unknown multicast storm control.									
<i>disable</i>	Disable unknown multicast storm control.									
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unknown unicast storm control.</td></tr><tr><td><i>disable</i></td><td>Disable unknown unicast storm control.</td></tr></table>	Option	Description	<i>enable</i>	Enable unknown unicast storm control.	<i>disable</i>	Disable unknown unicast storm control.			
Option	Description									
<i>enable</i>	Enable unknown unicast storm control.									
<i>disable</i>	Disable unknown unicast storm control.									

config switch-controller storm-control-policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch storm control policy to be applied on managed-switch ports.

```
config switch-controller storm-control-policy
  Description: Configure FortiSwitch storm control policy to be applied on managed-switch ports.
  edit <name>
    set broadcast [enable|disable]
    set description {string}
    set rate {integer}
    set storm-control-mode [global|override|...]
    set unknown-multicast [enable|disable]
    set unknown-unicast [enable|disable]
  next
end
```

config switch-controller storm-control-policy

Parameter	Description	Type	Size	Default
broadcast	Enable/disable storm control to drop/allow broadcast traffic in override mode.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.</td></tr><tr><td><i>disable</i></td><td>Disable storm control for broadcast traffic to allow all packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.					
	Option	Description										
	<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.										
<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.											
description	Description of the storm control policy.	string	Maximum length: 63									
name	Storm control policy name.	string	Maximum length: 63									
rate	Threshold rate in packets per second at which storm traffic is controlled in override mode (default=500, 0 to drop all).	integer	Minimum value: 0 Maximum value: 10000000	500								
storm-control-mode	Set Storm control mode.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Apply Global or switch level storm control configuration.</td></tr><tr><td><i>override</i></td><td>Override global and switch level storm control to use port level configuration.</td></tr><tr><td><i>disabled</i></td><td>Disable storm control on the port entirely overriding global and switch level storm control.</td></tr></table>	Option	Description	<i>global</i>	Apply Global or switch level storm control configuration.	<i>override</i>	Override global and switch level storm control to use port level configuration.	<i>disabled</i>	Disable storm control on the port entirely overriding global and switch level storm control.			
	Option	Description										
	<i>global</i>	Apply Global or switch level storm control configuration.										
	<i>override</i>	Override global and switch level storm control to use port level configuration.										
<i>disabled</i>	Disable storm control on the port entirely overriding global and switch level storm control.											
unknown-multicast	Enable/disable storm control to drop/allow unknown multicast traffic in override mode.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.</td></tr><tr><td><i>disable</i></td><td>Disable storm control for unknown multicast traffic to allow all packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for unknown multicast traffic to allow all packets.					
	Option	Description										
	<i>enable</i>	Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.										
<i>disable</i>	Disable storm control for unknown multicast traffic to allow all packets.											
unknown-unicast	Enable/disable storm control to drop/allow unknown unicast traffic in override mode.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.</td></tr><tr><td><i>disable</i></td><td>Disable storm control for unknown unicast traffic to allow all packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for unknown unicast traffic to allow all packets.					
	Option	Description										
	<i>enable</i>	Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.										
<i>disable</i>	Disable storm control for unknown unicast traffic to allow all packets.											

config switch-controller stp-instance



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.

```
config switch-controller stp-instance
  Description: Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.
  edit <id>
    set vlan-range <vlan-name1>, <vlan-name2>, ...
  next
end
```

config switch-controller stp-instance

Parameter	Description	Type	Size	Default
id	Instance ID.	string	Maximum length: 2	
vlan-range <vlan-name>	Configure VLAN range for STP instance. VLAN name.	string	Maximum length: 79	

config switch-controller stp-settings



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch spanning tree protocol (STP).

```
config switch-controller stp-settings
  Description: Configure FortiSwitch spanning tree protocol (STP).
  set forward-time {integer}
  set hello-time {integer}
  set max-age {integer}
  set max-hops {integer}
  set name {string}
  set pending-timer {integer}
  set revision {integer}
end
```

config switch-controller stp-settings

Parameter	Description	Type	Size	Default
forward-time	Period of time a port is in listening and learning state (4 - 30 sec, default = 15).	integer	Minimum value: 4 Maximum value: 30	15

Parameter	Description	Type	Size	Default
hello-time	Period of time between successive STP frame Bridge Protocol Data Units (BPDUs) sent on a port (1 - 10 sec, default = 2).	integer	Minimum value: 1 Maximum value: 10	2
max-age	Maximum time before a bridge port expires its configuration BPDU information (6 - 40 sec, default = 20).	integer	Minimum value: 6 Maximum value: 40	20
max-hops	Maximum number of hops between the root bridge and the furthest bridge (1- 40, default = 20).	integer	Minimum value: 1 Maximum value: 40	20
name	Name of global STP settings configuration.	string	Maximum length: 31	
pending-timer	Pending time (1 - 15 sec, default = 4).	integer	Minimum value: 1 Maximum value: 15	4
revision	STP revision number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535	0

config switch-controller switch-group



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch switch groups.

```
config switch-controller switch-group
  Description: Configure FortiSwitch switch groups.
  edit <name>
    set description {string}
    set fortilink {string}
    set members <switch-id1>, <switch-id2>, ...
  next
end
```

config switch-controller switch-group

Parameter	Description	Type	Size	Default
description	Optional switch group description.	string	Maximum length: 63	
fortilink	FortiLink interface to which switch group members belong.	string	Maximum length: 15	
members <switch-id>	FortiSwitch members belonging to this switch group.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
	Managed device ID.			
name	Switch group name.	string	Maximum length: 35	

config switch-controller switch-interface-tag



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure switch object tags.

```
config switch-controller switch-interface-tag
    Description: Configure switch object tags.
    edit <name>
        next
    end
```

config switch-controller switch-interface-tag

Parameter	Description	Type	Size	Default
name	Tag name.	string	Maximum length: 63	

config switch-controller switch-log



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch logging (logs are transferred to and inserted into FortiGate event log).

```
config switch-controller switch-log
    Description: Configure FortiSwitch logging (logs are transferred to and inserted into
FortiGate event log).
    set severity [emergency|alert|...]
    set status [enable|disable]
end
```

config switch-controller switch-log

Parameter	Description	Type	Size	Default
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-	notification
		Option	Description	
		emergency	Emergency level.	
		alert	Alert level.	

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																
	<i>critical</i>	Critical level.																
	<i>error</i>	Error level.																
	<i>warning</i>	Warning level.																
	<i>notification</i>	Notification level.																
	<i>information</i>	Information level.																
<i>debug</i>	Debug level.																	
status	Enable/disable adding FortiSwitch logs to FortiGate event log.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Add FortiSwitch logs to FortiGate event log.</td></tr><tr><td><i>disable</i></td><td>Do not add FortiSwitch logs to FortiGate event log.</td></tr></table>	Option	Description	<i>enable</i>	Add FortiSwitch logs to FortiGate event log.	<i>disable</i>	Do not add FortiSwitch logs to FortiGate event log.											
	Option	Description																
	<i>enable</i>	Add FortiSwitch logs to FortiGate event log.																
<i>disable</i>	Do not add FortiSwitch logs to FortiGate event log.																	

config switch-controller switch-profile



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch switch profile.

```

config switch-controller switch-profile
  Description: Configure FortiSwitch switch profile.
  edit <name>
    set login [enable|disable]
    set login-passwd {password}
    set login-passwd-override [enable|disable]
    set revision-backup-on-logout [enable|disable]
    set revision-backup-on-upgrade [enable|disable]
  next
end

```

config switch-controller switch-profile

Parameter	Description	Type	Size	Default						
login	Enable/disable FortiSwitch serial console.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiSwitch serial console.</td></tr><tr><td>disable</td><td>Disable FortiSwitch serial console.</td></tr></table>	Option	Description	enable	Enable FortiSwitch serial console.	disable	Disable FortiSwitch serial console.			
Option	Description									
enable	Enable FortiSwitch serial console.									
disable	Disable FortiSwitch serial console.									
login-passwd	Login password of managed FortiSwitch.	password	Not Specified							
login-passwd-override	Enable/disable overriding the admin administrator password for a managed FortiSwitch with the FortiGate admin administrator account password.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override a managed FortiSwitch's admin administrator password.</td></tr><tr><td>disable</td><td>Use the managed FortiSwitch admin administrator account password.</td></tr></table>	Option	Description	enable	Override a managed FortiSwitch's admin administrator password.	disable	Use the managed FortiSwitch admin administrator account password.			
Option	Description									
enable	Override a managed FortiSwitch's admin administrator password.									
disable	Use the managed FortiSwitch admin administrator account password.									
name	FortiSwitch Profile name.	string	Maximum length: 35							
revision-backup-on-logout	Enable/disable automatic revision backup upon logout from FortiSwitch.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable automatic revision backup upon logout from FortiSwitch.</td></tr><tr><td>disable</td><td>Disable automatic revision backup upon logout from FortiSwitch.</td></tr></table>	Option	Description	enable	Enable automatic revision backup upon logout from FortiSwitch.	disable	Disable automatic revision backup upon logout from FortiSwitch.			
Option	Description									
enable	Enable automatic revision backup upon logout from FortiSwitch.									
disable	Disable automatic revision backup upon logout from FortiSwitch.									
revision-backup-on-upgrade	Enable/disable automatic revision backup upon FortiSwitch image upgrade.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable automatic revision backup upon FortiSwitch image upgrade.		
	disable	Disable automatic revision backup upon FortiSwitch image upgrade.		

config switch-controller system



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R. It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure system-wide switch controller settings.

```
config switch-controller system
  Description: Configure system-wide switch controller settings.
  set caputp-echo-interval {integer}
  set caputp-max-retransmit {integer}
  set data-sync-interval {integer}
  set dynamic-periodic-interval {integer}
  set iot-holdoff {integer}
  set iot-mac-idle {integer}
  set iot-scan-interval {integer}
  set iot-weight-threshold {integer}
  set nac-periodic-interval {integer}
  set parallel-process {integer}
  set parallel-process-override [disable|enable]
```

```
set tunnel-mode [compatible|moderate|...]
end
```

config switch-controller system

Parameter	Description	Type	Size	Default
caputp-echo-interval	Echo interval for the caputp echo requests from swtp.	integer	Minimum value: 8 Maximum value: 600	30
caputp-max-retransmit	Maximum retransmission count for the caputp tunnel packets.	integer	Minimum value: 0 Maximum value: 64	5
data-sync-interval	Time interval between collection of switch data (30 - 1800 sec, default = 60, 0 = disable).	integer	Minimum value: 30 Maximum value: 1800	60
dynamic-periodic-interval	Periodic time interval to run Dynamic port policy engine (5 - 180 sec, default = 60).	integer	Minimum value: 5 Maximum value: 180	60
iot-holdoff	MAC entry's creation time. Time must be greater than this value for an entry to be created (0 - 10080 mins, default = 5 mins).	integer	Minimum value: 0 Maximum value: 10080	5
iot-mac-idle	MAC entry's idle time. MAC entry is removed after this value (0 - 10080 mins, default = 1440 mins).	integer	Minimum value: 0 Maximum value: 10080	1440
iot-scan-interval	IoT scan interval (2 - 10080 mins, default = 60 mins, 0 = disable).	integer	Minimum value: 2 Maximum value: 10080	60
iot-weight-threshold	MAC entry's confidence value. Value is queried when below this value (default = 1, 0 = disable).	integer	Minimum value: 0 Maximum value: 255	1

Parameter	Description	Type	Size	Default								
nac-periodic-interval	Periodic time interval to run NAC engine (5 - 180 sec, default = 60).	integer	Minimum value: 5 Maximum value: 180	60								
parallel-process	Maximum number of parallel processes.	integer	Minimum value: 1 Maximum value: 128 **	1								
parallel-process-override	Enable/disable parallel process override.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable maximum parallel process override.</td></tr><tr><td>enable</td><td>Enable maximum parallel process override.</td></tr></table>				Option	Description	disable	Disable maximum parallel process override.	enable	Enable maximum parallel process override.		
Option	Description											
disable	Disable maximum parallel process override.											
enable	Enable maximum parallel process override.											
tunnel-mode	Compatible/strict tunnel mode.	option	-	compatible								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>compatible</td><td>Least restrictive. Supports the lowest levels of security but highest compatibility between all FortiSwitch and FortiGate devices. 3rd party certificates permitted.</td></tr><tr><td>moderate</td><td>Moderate level of security. 3rd party certificates permitted.</td></tr><tr><td>strict</td><td>Highest level of security requirements. If enabled, the FortiGate device follows the same security mode requirements as in FIPS/CC mode.</td></tr></table>				Option	Description	compatible	Least restrictive. Supports the lowest levels of security but highest compatibility between all FortiSwitch and FortiGate devices. 3rd party certificates permitted.	moderate	Moderate level of security. 3rd party certificates permitted.	strict	Highest level of security requirements. If enabled, the FortiGate device follows the same security mode requirements as in FIPS/CC mode.
Option	Description											
compatible	Least restrictive. Supports the lowest levels of security but highest compatibility between all FortiSwitch and FortiGate devices. 3rd party certificates permitted.											
moderate	Moderate level of security. 3rd party certificates permitted.											
strict	Highest level of security requirements. If enabled, the FortiGate device follows the same security mode requirements as in FIPS/CC mode.											

** Values may differ between models.

config switch-controller traffic-policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch traffic policy.

```
config switch-controller traffic-policy
  Description: Configure FortiSwitch traffic policy.
  edit <name>
    set cos-queue {integer}
    set description {string}
    set guaranteed-bandwidth {integer}
    set guaranteed-burst {integer}
    set maximum-burst {integer}
    set policer-status [enable|disable]
    set type [ingress|egress]
  next
end
```

config switch-controller traffic-policy

Parameter	Description	Type	Size	Default						
cos-queue	COS queue(0 - 7), or unset to disable.	integer	Minimum value: 0 Maximum value: 7							
description	Description of the traffic policy.	string	Maximum length: 63							
guaranteed-bandwidth	Guaranteed bandwidth in kbps (max value = 524287000).	integer	Minimum value: 0 Maximum value: 524287000	10000						
guaranteed-burst	Guaranteed burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	45000						
maximum-burst	Maximum burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	67500						
name	Traffic policy name.	string	Maximum length: 63							
policer-status	Enable/disable policer config on the traffic policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable policer config on the traffic policy.</td></tr><tr><td>disable</td><td>Disable policer config on the traffic policy.</td></tr></table>				Option	Description	enable	Enable policer config on the traffic policy.	disable	Disable policer config on the traffic policy.
Option	Description									
enable	Enable policer config on the traffic policy.									
disable	Disable policer config on the traffic policy.									
type	Configure type of policy(ingress/egress). Read-only.	option	-	ingress						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ingress</td><td>Ingress policy.</td></tr><tr><td>egress</td><td>Egress policy.</td></tr></table>				Option	Description	ingress	Ingress policy.	egress	Egress policy.
Option	Description									
ingress	Ingress policy.									
egress	Egress policy.									

config switch-controller traffic-sniffer



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.

```
config switch-controller traffic-sniffer
  Description: Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.
  set erspan-ip {ipv4-address}
  set mode [erspan-auto|rspan|...]
  config target-ip
    Description: Sniffer IPs to filter.
    edit <ip>
      set description {string}
    next
  end
  config target-mac
    Description: Sniffer MACs to filter.
    edit <mac>
      set description {string}
    next
  end
  config target-port
    Description: Sniffer ports to filter.
    edit <switch-id>
      set description {string}
      set in-ports <name1>, <name2>, ...
      set out-ports <name1>, <name2>, ...
```

```
    next
end
end
```

config switch-controller traffic-sniffer

Parameter	Description	Type	Size	Default
erspan-ip	Configure ERSPAN collector IP address.	ipv4-address	Not Specified	0.0.0.0
mode	Configure traffic sniffer mode.	option	-	erspan-auto
	Option	Description		
	<i>erspan-auto</i>	Mirror traffic using a GRE tunnel.		
	<i>rspan</i>	Mirror traffic on a layer2 VLAN.		
	<i>none</i>	Disable traffic mirroring (sniffer).		

config target-ip

Parameter	Description	Type	Size	Default
description	Description for the sniffer IP.	string	Maximum length: 63	
ip	Sniffer IP.	ipv4-address	Not Specified	0.0.0.0

config target-mac

Parameter	Description	Type	Size	Default
description	Description for the sniffer MAC.	string	Maximum length: 63	
mac	Sniffer MAC.	mac-address	Not Specified	00:00:00:00:00:00

config target-port

Parameter	Description	Type	Size	Default
description	Description for the sniffer port entry.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
in-ports <name>	Configure source ingress port interfaces. Interface name.	string	Maximum length: 79	
out-ports <name>	Configure source egress port interfaces. Interface name.	string	Maximum length: 79	
switch-id	Managed-switch ID.	string	Maximum length: 16	

config switch-controller virtual-port-pool



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure virtual pool.

```
config switch-controller virtual-port-pool
  Description: Configure virtual pool.
  edit <name>
    set description {string}
  next
end
```


config switch-controller virtual-port-pool

Parameter	Description	Type	Size	Default
description	Virtual switch pool description.	string	Maximum length: 63	
name	Virtual switch pool name.	string	Maximum length: 35	

config switch-controller vlan-policy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure VLAN policy to be applied on the managed FortiSwitch ports through dynamic-port-policy.

```
config switch-controller vlan-policy
    Description: Configure VLAN policy to be applied on the managed FortiSwitch ports through
dynamic-port-policy.
    edit <name>
        set allowed-vlans <vlan-name1>, <vlan-name2>, ...
        set allowed-vlans-all [enable|disable]
        set description {string}
        set discard-mode [none|all-untagged|...]
        set fortalink {string}
        set untagged-vlans <vlan-name1>, <vlan-name2>, ...
```

```

        set vlan {string}
    next
end

```

config switch-controller vlan-policy

Parameter	Description	Type	Size	Default								
allowed-vlans <vlan-name>	Allowed VLANs to be applied when using this VLAN policy. VLAN name.	string	Maximum length: 79									
allowed-vlans-all	Enable/disable all defined VLANs when using this VLAN policy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable all defined VLANs.</td></tr><tr><td><i>disable</i></td><td>Disable all defined VLANs.</td></tr></table>	Option	Description	<i>enable</i>	Enable all defined VLANs.	<i>disable</i>	Disable all defined VLANs.					
Option	Description											
<i>enable</i>	Enable all defined VLANs.											
<i>disable</i>	Disable all defined VLANs.											
description	Description for the VLAN policy.	string	Maximum length: 63									
discard-mode	Discard mode to be applied when using this VLAN policy.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Discard disabled.</td></tr><tr><td><i>all-untagged</i></td><td>Discard all frames that are untagged.</td></tr><tr><td><i>all-tagged</i></td><td>Discard all frames that are tagged.</td></tr></table>	Option	Description	<i>none</i>	Discard disabled.	<i>all-untagged</i>	Discard all frames that are untagged.	<i>all-tagged</i>	Discard all frames that are tagged.			
Option	Description											
<i>none</i>	Discard disabled.											
<i>all-untagged</i>	Discard all frames that are untagged.											
<i>all-tagged</i>	Discard all frames that are tagged.											
fortilink	FortiLink interface for which this VLAN policy belongs to.	string	Maximum length: 15									
name	VLAN policy name.	string	Maximum length: 63									
untagged-vlans <vlan-name>	Untagged VLANs to be applied when using this VLAN policy. VLAN name.	string	Maximum length: 79									
vlan	Native VLAN to be applied when using this VLAN policy.	string	Maximum length: 15									

system

This section includes syntax for the following commands:

- [config system 3g-modem custom on page 1327](#)
- [config system accprofile on page 1328](#)
- [config system acme on page 1340](#)
- [config system admin on page 1342](#)
- [config system affinity-interrupt on page 1349](#)
- [config system affinity-packet-redistribution on page 1350](#)
- [config system alarm on page 1351](#)
- [config system alias on page 1354](#)
- [config system api-user on page 1354](#)
- [config system arp-table on page 1356](#)
- [config system auto-install on page 1374](#)
- [config system auto-scale on page 1375](#)
- [config system auto-script on page 1376](#)
- [config system automation-action on page 1357](#)
- [config system automation-condition on page 1363](#)
- [config system automation-destination on page 1365](#)
- [config system automation-stitch on page 1365](#)
- [config system automation-trigger on page 1367](#)
- [config system autoupdate schedule on page 1372](#)
- [config system autoupdate tunneling on page 1373](#)
- [config system bypass on page 1378](#)
- [config system central-management on page 1379](#)
- [config system cloud-service on page 1385](#)
- [config system console on page 1386](#)
- [config system csf on page 1387](#)
- [config system custom-language on page 1393](#)
- [config system ddns on page 1393](#)
- [config system dedicated-mgmt on page 1396](#)
- [config system device-upgrade on page 1397](#)
- [config system dhcp6 server on page 1412](#)
- [config system dhcp server on page 1401](#)
- [config system digital-io on page 1418](#)
- [config system dnp3-proxy on page 1419](#)
- [config system dns-database on page 1425](#)
- [config system dns-server on page 1429](#)
- [config system dns on page 1421](#)

-
- [config system dns64 on page 1424](#)
 - [config system dscp-based-priority on page 1430](#)
 - [config system elbc on page 1432](#)
 - [config system email-server on page 1433](#)
 - [config system evpn on page 1435](#)
 - [config system external-resource on page 1436](#)
 - [config system fabric-vpn on page 1440](#)
 - [config system federated-upgrade on page 1444](#)
 - [config system fips-cc on page 1449](#)
 - [config system fortiguard on page 1450](#)
 - [config system fortindr on page 1460](#)
 - [config system fortisandbox on page 1461](#)
 - [config system fsso-polling on page 1463](#)
 - [config system ftm-push on page 1464](#)
 - [config system geneve on page 1465](#)
 - [config system geoip-override on page 1466](#)
 - [config system global on page 1468](#)
 - [config system gre-tunnel on page 1517](#)
 - [config system ha-monitor on page 1534](#)
 - [config system ha on page 1519](#)
 - [config system health-check-fortiguard on page 1535](#)
 - [config system icond on page 1536](#)
 - [config system ike on page 1541](#)
 - [config system interface on page 1554](#)
 - [config system ipam on page 1625](#)
 - [config system ipip-tunnel on page 1628](#)
 - [config system ips-urlfilter-dns on page 1631](#)
 - [config system ips-urlfilter-dns6 on page 1632](#)
 - [config system ips on page 1629](#)
 - [config system ipsec-aggregate on page 1630](#)
 - [config system ipv6-neighbor-cache on page 1632](#)
 - [config system ipv6-tunnel on page 1633](#)
 - [config system iscsi on page 1634](#)
 - [config system isf-queue-profile on page 1636](#)
 - [config system link-monitor on page 1638](#)
 - [config system lldp network-policy on page 1643](#)
 - [config system lte-modem on page 1651](#)
 - [config system mac-address-table on page 1659](#)
 - [config system management-tunnel on page 1660](#)
 - [config system mobile-tunnel on page 1661](#)
 - [config system modem on page 1664](#)
 - [config system nd-proxy on page 1671](#)
 - [config system netflow on page 1672](#)

-
- [config system network-visibility on page 1674](#)
 - [config system ngfw-settings on page 1675](#)
 - [config system np6 on page 1676](#)
 - [config system np6xlite on page 1689](#)
 - [config system npu-post on page 1797](#)
 - [config system npu-setting prp on page 1798](#)
 - [config system npu-vlink on page 1799](#)
 - [config system npu on page 1703](#)
 - [config system ntp on page 1800](#)
 - [config system object-tagging on page 1803](#)
 - [config system password-policy-guest-admin on page 1807](#)
 - [config system password-policy on page 1805](#)
 - [config system pcp-server on page 1809](#)
 - [config system physical-switch on page 1812](#)
 - [config system pppoe-interface on page 1813](#)
 - [config system probe-response on page 1816](#)
 - [config system proxy-arp on page 1817](#)
 - [config system ptp on page 1818](#)
 - [config system replacemsg-group on page 1837](#)
 - [config system replacemsg-image on page 1850](#)
 - [config system replacemsg admin on page 1819](#)
 - [config system replacemsg alertmail on page 1820](#)
 - [config system replacemsg auth on page 1821](#)
 - [config system replacemsg automation on page 1822](#)
 - [config system replacemsg custom-message on page 1823](#)
 - [config system replacemsg fortiguard-wf on page 1824](#)
 - [config system replacemsg ftp on page 1826](#)
 - [config system replacemsg http on page 1827](#)
 - [config system replacemsg icap on page 1828](#)
 - [config system replacemsg mail on page 1829](#)
 - [config system replacemsg nac-quar on page 1830](#)
 - [config system replacemsg spam on page 1831](#)
 - [config system replacemsg sslvpn on page 1832](#)
 - [config system replacemsg traffic-quota on page 1833](#)
 - [config system replacemsg utm on page 1834](#)
 - [config system replacemsg webproxy on page 1836](#)
 - [config system resource-limits on page 1850](#)
 - [config system saml on page 1853](#)
 - [config system sdn-connector on page 1857](#)
 - [config system sdn-proxy on page 1866](#)
 - [config system sdn-vpn on page 1867](#)
 - [config system sdwan on page 1869](#)
 - [config system security-rating controls on page 1895](#)

-
- [config system security-rating settings on page 1896](#)
 - [config system serial-port on page 1897](#)
 - [config system session-helper on page 1898](#)
 - [config system session-ttl on page 1899](#)
 - [config system settings on page 1900](#)
 - [config system sflow on page 1926](#)
 - [config system sit-tunnel on page 1927](#)
 - [config system smc-ntp on page 1929](#)
 - [config system sms-server on page 1930](#)
 - [config system snmp community on page 1931](#)
 - [config system snmp mib-view on page 1940](#)
 - [config system snmp rmon-stat on page 1941](#)
 - [config system snmp sysinfo on page 1942](#)
 - [config system snmp user on page 1944](#)
 - [config system speed-test-schedule on page 1951](#)
 - [config system speed-test-server on page 1954](#)
 - [config system speed-test-setting on page 1955](#)
 - [config system ssh-config on page 1956](#)
 - [config system sso-admin on page 1960](#)
 - [config system sso-forticloud-admin on page 1960](#)
 - [config system sso-fortigate-cloud-admin on page 1961](#)
 - [config system standalone-cluster on page 1961](#)
 - [config system storage on page 1966](#)
 - [config system stp on page 1968](#)
 - [config system switch-interface on page 1969](#)
 - [config system timezone on page 1971](#)
 - [config system tos-based-priority on page 1972](#)
 - [config system vdom-dns on page 1973](#)
 - [config system vdom-exception on page 1975](#)
 - [config system vdom-link on page 1977](#)
 - [config system vdom-netflow on page 1978](#)
 - [config system vdom-property on page 1980](#)
 - [config system vdom-radius-server on page 1982](#)
 - [config system vdom-sflow on page 1982](#)
 - [config system vdom on page 1973](#)
 - [config system vin-alarm on page 1984](#)
 - [config system virtual-switch on page 1986](#)
 - [config system virtual-wire-pair on page 1988](#)
 - [config system vne-interface on page 1989](#)
 - [config system vpce on page 1991](#)
 - [config system vxlan on page 1992](#)
 - [config system wccp on page 1993](#)
 - [config system wireless ap-status on page 1998](#)

- [config system wireless settings on page 1999](#)
- [config system zone on page 2002](#)

config system 3g-modem custom



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

3G MODEM custom.

```
config system 3g-modem custom
  Description: 3G MODEM custom.
  edit <id>
    set class-id {user}
    set init-string {string}
    set model {string}
    set modeswitch-string {string}
    set product-id {user}
    set vendor {string}
    set vendor-id {user}
  next
end
```

config system 3g-modem custom

Parameter	Description	Type	Size	Default
class-id	USB interface class in hexadecimal format (00-ff).	user	Not Specified	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
init-string	Init string in hexadecimal format (even length).	string	Maximum length: 127	
model	MODEM model name.	string	Maximum length: 35	
modeswitch-string	USB modeswitch arguments. For example: '-v 1410 -p 9030 -V 1410 -P 9032 -u 3'.	string	Maximum length: 127	
product-id	USB product ID in hexadecimal format (0000-ffff).	user	Not Specified	
vendor	MODEM vendor name.	string	Maximum length: 35	
vendor-id	USB vendor ID in hexadecimal format (0000-ffff).	user	Not Specified	

config system accprofile

Configure access profiles for system administrators.

```
config system accprofile
  Description: Configure access profiles for system administrators.
  edit <name>
    set admintimeout {integer}
    set admintimeout-override [enable|disable]
    set authgrp [none|read|...]
    set cli-config [enable|disable]
    set cli-diagnose [enable|disable]
    set cli-exec [enable|disable]
    set cli-get [enable|disable]
    set cli-show [enable|disable]
    set comments {var-string}
    set ftviewgrp [none|read|...]
    set fwgrp [none|read|...]
    config fwgrp-permission
      Description: Custom firewall permission.
      set address [none|read|...]
```



```

    set others [none|read|...]
    set policy [none|read|...]
    set schedule [none|read|...]
    set service [none|read|...]
end
set loggrp [none|read|...]
config loggrp-permission
    Description: Custom Log & Report permission.
    set config [none|read|...]
    set data-access [none|read|...]
    set report-access [none|read|...]
    set threat-weight [none|read|...]
end
set netgrp [none|read|...]
config netgrp-permission
    Description: Custom network permission.
    set cfg [none|read|...]
    set packet-capture [none|read|...]
    set route-cfg [none|read|...]
end
set scope [vdom|global]
set secfabgrp [none|read|...]
set sysgrp [none|read|...]
config sysgrp-permission
    Description: Custom system permission.
    set admin [none|read|...]
    set cfg [none|read|...]
    set mnt [none|read|...]
    set upd [none|read|...]
end
set system-execute-ssh [enable|disable]
set system-execute-telnet [enable|disable]
set utmgrp [none|read|...]
config utmgrp-permission
    Description: Custom Security Profile permissions.
    set antivirus [none|read|...]
    set application-control [none|read|...]
    set casb [none|read|...]
    set dlp [none|read|...]
    set dnsfilter [none|read|...]
    set emailfilter [none|read|...]
    set endpoint-control [none|read|...]
    set file-filter [none|read|...]
    set icap [none|read|...]
    set ips [none|read|...]
    set videofilter [none|read|...]
    set virtual-patch [none|read|...]
    set voip [none|read|...]
    set waf [none|read|...]
    set webfilter [none|read|...]
end
set vpngrp [none|read|...]

```

```

        set wanoptgrp [none|read|...]
        set wifi [none|read|...]
    next
end

```

config system accprofile

Parameter	Description	Type	Size	Default								
admintimeout	Administrator timeout for this access profile (0 - 480 min, default = 10, 0 means never timeout).	integer	Minimum value: 1 Maximum value: 480	10								
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable overriding the global administrator idle timeout.</td></tr><tr><td>disable</td><td>Disable overriding the global administrator idle timeout.</td></tr></table>	Option	Description	enable	Enable overriding the global administrator idle timeout.	disable	Disable overriding the global administrator idle timeout.					
Option	Description											
enable	Enable overriding the global administrator idle timeout.											
disable	Disable overriding the global administrator idle timeout.											
authgrp	Administrator access to Users and Devices.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No access.</td></tr><tr><td>read</td><td>Read access.</td></tr><tr><td>read-write</td><td>Read/write access.</td></tr></table>	Option	Description	none	No access.	read	Read access.	read-write	Read/write access.			
Option	Description											
none	No access.											
read	Read access.											
read-write	Read/write access.											
cli-config	Enable/disable permission to run config commands.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable permission to run config commands.</td></tr><tr><td>disable</td><td>Disable permission to run config commands.</td></tr></table>	Option	Description	enable	Enable permission to run config commands.	disable	Disable permission to run config commands.					
Option	Description											
enable	Enable permission to run config commands.											
disable	Disable permission to run config commands.											
cli-diagnose	Enable/disable permission to run diagnostic commands.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable permission to run diagnostic commands.</td></tr><tr><td>disable</td><td>Disable permission to run diagnostic commands.</td></tr></table>	Option	Description	enable	Enable permission to run diagnostic commands.	disable	Disable permission to run diagnostic commands.					
Option	Description											
enable	Enable permission to run diagnostic commands.											
disable	Disable permission to run diagnostic commands.											
cli-exec	Enable/disable permission to run execute commands.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable permission to run execute commands.		
	<i>disable</i>	Disable permission to run execute commands.		
cli-get	Enable/disable permission to run get commands.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable permission to run get commands.		
	<i>disable</i>	Disable permission to run get commands.		
cli-show	Enable/disable permission to run show commands.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable permission to run show commands.		
	<i>disable</i>	Disable permission to run show commands.		
comments	Comment.	var-string	Maximum length: 255	
ftviewgrp	FortiView.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
fwgrp	Administrator access to the Firewall configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
loggrp	Administrator access to Logging and Reporting including viewing log messages.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
name	Profile name.	string	Maximum length: 35	
netgrp	Network Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
scope	Scope of admin access: global or specific VDOM (s).	option	-	vdom
	Option	Description		
	<i>vdom</i>	VDOM access.		
	<i>global</i>	Global access.		
secfabgrp	Security Fabric.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
sysgrp	System Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		

Parameter	Description	Type	Size	Default										
system-execute-ssh	Enable/disable permission to execute SSH commands.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable permission to execute SSH commands.</td></tr><tr><td>disable</td><td>Disable permission to execute SSH commands.</td></tr></table>	Option	Description	enable	Enable permission to execute SSH commands.	disable	Disable permission to execute SSH commands.							
Option	Description													
enable	Enable permission to execute SSH commands.													
disable	Disable permission to execute SSH commands.													
system-execute-telnet	Enable/disable permission to execute TELNET commands.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable permission to execute TELNET commands.</td></tr><tr><td>disable</td><td>Disable permission to execute TELNET commands.</td></tr></table>	Option	Description	enable	Enable permission to execute TELNET commands.	disable	Disable permission to execute TELNET commands.							
Option	Description													
enable	Enable permission to execute TELNET commands.													
disable	Disable permission to execute TELNET commands.													
utmgrp	Administrator access to Security Profiles.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No access.</td></tr><tr><td>read</td><td>Read access.</td></tr><tr><td>read-write</td><td>Read/write access.</td></tr><tr><td>custom</td><td>Customized access.</td></tr></table>	Option	Description	none	No access.	read	Read access.	read-write	Read/write access.	custom	Customized access.			
Option	Description													
none	No access.													
read	Read access.													
read-write	Read/write access.													
custom	Customized access.													
vpngrp	Administrator access to IPsec, SSL, PPTP, and L2TP VPN.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No access.</td></tr><tr><td>read</td><td>Read access.</td></tr><tr><td>read-write</td><td>Read/write access.</td></tr></table>	Option	Description	none	No access.	read	Read access.	read-write	Read/write access.					
Option	Description													
none	No access.													
read	Read access.													
read-write	Read/write access.													
wanoptgrp *	Administrator access to WAN Opt & Cache.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No access.</td></tr><tr><td>read</td><td>Read access.</td></tr><tr><td>read-write</td><td>Read/write access.</td></tr></table>	Option	Description	none	No access.	read	Read access.	read-write	Read/write access.					
Option	Description													
none	No access.													
read	Read access.													
read-write	Read/write access.													
wifi	Administrator access to the WiFi controller and Switch controller.	option	-	none										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

* This parameter may not exist in some models.

config fwgrp-permission

Parameter	Description	Type	Size	Default
address	Address Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
others	Other Firewall Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
policy	Policy Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
schedule	Schedule Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

Parameter	Description	Type	Size	Default
service	Service Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config loggrp-permission

Parameter	Description	Type	Size	Default
config	Log & Report configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
data-access	Log & Report Data Access.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
report-access	Log & Report Report Access.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
threat-weight	Log & Report Threat Weight.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config netgrp-permission

Parameter	Description	Type	Size	Default
cfg	Network Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
packet-capture	Packet Capture Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
route-cfg	Router Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config sysgrp-permission

Parameter	Description	Type	Size	Default
admin	Administrator Users.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
cfg	System Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>read-write</i>	Read/write access.		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
mnt	Maintenance.	option	-	none
	Option	Description		
	<i>read-write</i>	Read/write access.		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
upd	FortiGuard Updates.	option	-	none
	Option	Description		
	<i>read-write</i>	Read/write access.		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		

config utmgrp-permission

Parameter	Description	Type	Size	Default
antivirus	Antivirus profiles and settings.	option	-	none
	Option	Description		
	<i>read-write</i>	Read/write access.		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
application-control	Application Control profiles and settings.	option	-	none
	Option	Description		
	<i>read-write</i>	Read/write access.		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
casb	Inline CASB filter profile and settings	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
dlp	DLP profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
dnsfilter	DNS Filter profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
emailfilter	Email Filter and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
endpoint-control	FortiClient Profiles.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
file-filter	File-filter profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
icap	ICAP profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
ips	IPS profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
videofilter	Video filter profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
virtual-patch	Virtual patch profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
voip	VoIP profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

Parameter	Description	Type	Size	Default								
waf	Web Application Firewall profiles and settings.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
webfilter	Web Filter profiles and settings.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

config system acme

Configure ACME client.

```

config system acme
  Description: Configure ACME client.
  config accounts
    Description: ACME accounts list.
    edit <id>
      set ca_url {string}
      set eab-key-hmac {password}
      set eab-key-id {var-string}
      set email {string}
      set privatekey {string}
      set status {string}
      set url {string}
    next
  end
  set interface <interface-name1>, <interface-name2>, ...
  set source-ip {ipv4-address}
  set source-ip6 {ipv6-address}
  set use-ha-direct [enable|disable]
end

```

config system acme

Parameter	Description	Type	Size	Default
interface <interface-name>	Interface(s) on which the ACME client will listen for challenges. Interface name.	string	Maximum length: 79	
source-ip	Source IPv4 address used to connect to the ACME server.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used to connect to the ACME server.	ipv6-address	Not Specified	::
use-ha-direct	Enable the use of 'ha-mgmt' interface to connect to the ACME server when 'ha-direct' is enabled in HA configuration	option	-	disable
		Option	Description	
		enable	Enable setting.	
		disable	Disable setting.	

config accounts

Parameter	Description	Type	Size	Default
ca_url	Account ca_url.	string	Maximum length: 255	
eab-key-hmac	External Account Binding Key HMAC.	password	Not Specified	
eab-key-id	External Account Binding Key ID.	var-string	Maximum length: 255	
email	Account email.	string	Maximum length: 255	
id	Account id.	string	Maximum length: 255	
privatekey	Account Private Key.	string	Maximum length: 8191	
status	Account status.	string	Maximum length: 127	
url	Account url.	string	Maximum length: 511	

config system admin

Configure admin users.

```
config system admin
  Description: Configure admin users.
  edit <name>
    set accprofile {string}
    set accprofile-override [enable|disable]
    set allow-remove-admin-session [enable|disable]
    set comments {var-string}
    set email-to {string}
    set force-password-change [enable|disable]
    set fortitoken {string}
    set guest-auth [disable|enable]
    set guest-lang {string}
    set guest-usergroups <name1>, <name2>, ...
    set ip6-trusthost1 {ipv6-prefix}
    set ip6-trusthost10 {ipv6-prefix}
    set ip6-trusthost2 {ipv6-prefix}
    set ip6-trusthost3 {ipv6-prefix}
    set ip6-trusthost4 {ipv6-prefix}
    set ip6-trusthost5 {ipv6-prefix}
    set ip6-trusthost6 {ipv6-prefix}
    set ip6-trusthost7 {ipv6-prefix}
    set ip6-trusthost8 {ipv6-prefix}
    set ip6-trusthost9 {ipv6-prefix}
    set password {password-2}
    set password-expire {datetime}
    set peer-auth [enable|disable]
    set peer-group {string}
    set remote-auth [enable|disable]
    set remote-group {string}
    set schedule {string}
    set sms-custom-server {string}
    set sms-phone {string}
    set sms-server [fortiguard|custom]
    set ssh-certificate {string}
    set ssh-public-key1 {user}
    set ssh-public-key2 {user}
    set ssh-public-key3 {user}
    set trusthost1 {ipv4-classnet}
    set trusthost10 {ipv4-classnet}
    set trusthost2 {ipv4-classnet}
    set trusthost3 {ipv4-classnet}
    set trusthost4 {ipv4-classnet}
    set trusthost5 {ipv4-classnet}
    set trusthost6 {ipv4-classnet}
    set trusthost7 {ipv4-classnet}
    set trusthost8 {ipv4-classnet}
    set trusthost9 {ipv4-classnet}
```

```

set two-factor [disable|fortitoken|...]
set two-factor-authentication [fortitoken|email|...]
set two-factor-notification [email|sms]
set vdom <name1>, <name2>, ...
set vdom-override [enable|disable]
set wildcard [enable|disable]
next
end

```

config system admin

Parameter	Description	Type	Size	Default						
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiGate features.	string	Maximum length: 35							
accprofile-override	Enable to use the name of an access profile provided by the remote authentication server to control the FortiGate features that this administrator can access.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable access profile override.</td></tr><tr><td><i>disable</i></td><td>Disable access profile override.</td></tr></table>	Option	Description	<i>enable</i>	Enable access profile override.	<i>disable</i>	Disable access profile override.			
Option	Description									
<i>enable</i>	Enable access profile override.									
<i>disable</i>	Disable access profile override.									
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allow-remove option.</td></tr><tr><td><i>disable</i></td><td>Disable allow-remove option.</td></tr></table>	Option	Description	<i>enable</i>	Enable allow-remove option.	<i>disable</i>	Disable allow-remove option.			
Option	Description									
<i>enable</i>	Enable allow-remove option.									
<i>disable</i>	Disable allow-remove option.									
comments	Comment.	var-string	Maximum length: 255							
email-to	This administrator's email address.	string	Maximum length: 63							
force-password-change	Enable/disable force password change on next login.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable force password change on next login.</td></tr><tr><td><i>disable</i></td><td>Disable force password change on next login.</td></tr></table>	Option	Description	<i>enable</i>	Enable force password change on next login.	<i>disable</i>	Disable force password change on next login.			
Option	Description									
<i>enable</i>	Enable force password change on next login.									
<i>disable</i>	Disable force password change on next login.									

Parameter	Description	Type	Size	Default						
fortitoken	This administrator's FortiToken serial number.	string	Maximum length: 16							
guest-auth	Enable/disable guest authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable guest authentication.</td></tr><tr><td>enable</td><td>Enable guest authentication.</td></tr></table>	Option	Description	disable	Disable guest authentication.	enable	Enable guest authentication.			
Option	Description									
disable	Disable guest authentication.									
enable	Enable guest authentication.									
guest-lang	Guest management portal language.	string	Maximum length: 35							
guest-usergroups <name>	Select guest user groups. Select guest user groups.	string	Maximum length: 79							
ip6-trusthost1	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost10	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost2	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost3	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost4	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost5	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost6	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						

Parameter	Description	Type	Size	Default						
ip6-trusthost7	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost8	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost9	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
name	User name.	string	Maximum length: 64							
password	Admin user password.	password-2	Not Specified							
password-expire	Password expire time.	datetime	Not Specified	0000-00-00 00:00:00						
peer-auth	Set to enable peer certificate authentication (for HTTPS admin access).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable peer.</td></tr><tr><td><i>disable</i></td><td>Disable peer.</td></tr></table>				Option	Description	<i>enable</i>	Enable peer.	<i>disable</i>	Disable peer.
Option	Description									
<i>enable</i>	Enable peer.									
<i>disable</i>	Disable peer.									
peer-group	Name of peer group defined under config user group which has PKI members. Used for peer certificate authentication (for HTTPS admin access).	string	Maximum length: 35							
remote-auth	Enable/disable authentication using a remote RADIUS, LDAP, or TACACS+ server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable remote authentication.</td></tr><tr><td><i>disable</i></td><td>Disable remote authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable remote authentication.	<i>disable</i>	Disable remote authentication.
Option	Description									
<i>enable</i>	Enable remote authentication.									
<i>disable</i>	Disable remote authentication.									
remote-group	User group name used for remote auth.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
schedule	Firewall schedule used to restrict when the administrator can log in. No schedule means no restrictions.	string	Maximum length: 35							
sms-custom-server	Custom SMS server to send SMS messages to.	string	Maximum length: 35							
sms-phone	Phone number on which the administrator receives SMS messages.	string	Maximum length: 15							
sms-server	Send SMS messages using the FortiGuard SMS server or a custom server.	option	-	fortiguard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fortiguard</td><td>Send SMS by FortiGuard.</td></tr><tr><td>custom</td><td>Send SMS by custom server.</td></tr></table>				Option	Description	fortiguard	Send SMS by FortiGuard.	custom	Send SMS by custom server.
Option	Description									
fortiguard	Send SMS by FortiGuard.									
custom	Send SMS by custom server.									
ssh-certificate	Select the certificate to be used by the FortiGate for authentication with an SSH client.	string	Maximum length: 35							
ssh-public-key1	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified							
ssh-public-key2	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified							
ssh-public-key3	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified							
trusthost1	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
trusthost10	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
trusthost2	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						

Parameter	Description	Type	Size	Default												
trusthost3	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost4	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost5	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost6	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost7	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost8	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost9	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
two-factor	Enable/disable two-factor authentication.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable two-factor authentication.</td></tr><tr><td>fortitoken</td><td>Use FortiToken or FortiToken mobile two-factor authentication.</td></tr><tr><td>fortitoken-cloud</td><td>FortiToken Cloud Service.</td></tr><tr><td>email</td><td>Send a two-factor authentication code to the configured email-to email address.</td></tr><tr><td>sms</td><td>Send a two-factor authentication code to the configured sms-server and sms-phone.</td></tr></table>				Option	Description	disable	Disable two-factor authentication.	fortitoken	Use FortiToken or FortiToken mobile two-factor authentication.	fortitoken-cloud	FortiToken Cloud Service.	email	Send a two-factor authentication code to the configured email-to email address.	sms	Send a two-factor authentication code to the configured sms-server and sms-phone.
Option	Description															
disable	Disable two-factor authentication.															
fortitoken	Use FortiToken or FortiToken mobile two-factor authentication.															
fortitoken-cloud	FortiToken Cloud Service.															
email	Send a two-factor authentication code to the configured email-to email address.															
sms	Send a two-factor authentication code to the configured sms-server and sms-phone.															

Parameter	Description	Type	Size	Default								
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortitoken</i></td><td>FortiToken authentication.</td></tr><tr><td><i>email</i></td><td>Email one time password.</td></tr><tr><td><i>sms</i></td><td>SMS one time password.</td></tr></table>	Option	Description	<i>fortitoken</i>	FortiToken authentication.	<i>email</i>	Email one time password.	<i>sms</i>	SMS one time password.			
Option	Description											
<i>fortitoken</i>	FortiToken authentication.											
<i>email</i>	Email one time password.											
<i>sms</i>	SMS one time password.											
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>email</i></td><td>Email notification for activation code.</td></tr><tr><td><i>sms</i></td><td>SMS notification for activation code.</td></tr></table>	Option	Description	<i>email</i>	Email notification for activation code.	<i>sms</i>	SMS notification for activation code.					
Option	Description											
<i>email</i>	Email notification for activation code.											
<i>sms</i>	SMS notification for activation code.											
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79									
vdom-override	Enable to use the names of VDOMs provided by the remote authentication server to control the VDOMs that this administrator can access.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VDOM override.</td></tr><tr><td><i>disable</i></td><td>Disable VDOM override.</td></tr></table>	Option	Description	<i>enable</i>	Enable VDOM override.	<i>disable</i>	Disable VDOM override.					
Option	Description											
<i>enable</i>	Enable VDOM override.											
<i>disable</i>	Disable VDOM override.											
wildcard	Enable/disable wildcard RADIUS authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable username wildcard.</td></tr><tr><td><i>disable</i></td><td>Disable username wildcard.</td></tr></table>	Option	Description	<i>enable</i>	Enable username wildcard.	<i>disable</i>	Disable username wildcard.					
Option	Description											
<i>enable</i>	Enable username wildcard.											
<i>disable</i>	Disable username wildcard.											

config system affinity-interrupt



This command is available for model(s): FortiGate 100F, FortiGate 101F, FortiGate 120G, FortiGate 121G, FortiGate 200F, FortiGate 201F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 1100E, FortiGate 1101E, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F.

Configure interrupt affinity.

```
config system affinity-interrupt
  Description: Configure interrupt affinity.
  edit <id>
    set affinity-cpumask {string}
    set default-affinity-cpumask {string}
    set interrupt {string}
  next
end
```

config system affinity-interrupt

Parameter	Description	Type	Size	Default
affinity-cpumask	Affinity setting (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127	
default-affinity-cpumask	Default affinity setting (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx). Read-only.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
id	ID of the interrupt affinity setting.	integer	Minimum value: 0 Maximum value: 4294967295	0
interrupt	Interrupt name.	string	Maximum length: 127	

config system affinity-packet-redistribution



This command is available for model(s): FortiGate 100F, FortiGate 101F, FortiGate 120G, FortiGate 121G, FortiGate 200F, FortiGate 201F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 1100E, FortiGate 1101E, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F.

Configure packet redistribution.

```
config system affinity-packet-redistribution
  Description: Configure packet redistribution.
  edit <id>
    set affinity-cpumask {string}
    set interface {string}
    set round-robin [enable|disable]
    set rxqid {integer}
  next
end
```

config system affinity-packet-redistribution

Parameter	Description	Type	Size	Default
affinity-cpumask	Hexadecimal cpumask, empty value means all CPUs.	string	Maximum length: 127	
id	ID of the packet redistribution setting.	integer	Minimum value: 0 Maximum value: 4294967295	
interface	Physical interface name on which to perform packet redistribution.	string	Maximum length: 15	
round-robin	Enable/disable round-robin redistribution to multiple CPUs.	option	-	enable
	Option	Description		
	enable	Enable round-robin redistribution.		
	disable	Disable round-robin redistribution.		
rxqid	ID of the receive queue (when the interface has multiple queues) on which to perform packet redistribution (255 = all queues).	integer	Minimum value: 0 Maximum value: 255	255

config system alarm

Configure alarm.

```
config system alarm
  Description: Configure alarm.
  set audible [enable|disable]
  config groups
    Description: Alarm groups.
    edit <id>
      set admin-auth-failure-threshold {integer}
      set admin-auth-lockout-threshold {integer}
      set decryption-failure-threshold {integer}
      set encryption-failure-threshold {integer}
      set fw-policy-id {integer}
      set fw-policy-id-threshold {integer}
    config fw-policy-violations
      Description: Firewall policy violations.
      edit <id>
        set dst-ip {ipv4-address}
        set dst-port {integer}
        set src-ip {ipv4-address}
        set src-port {integer}
```

```

        set threshold {integer}
    next
end
set log-full-warning-threshold {integer}
set period {integer}
set replay-attempt-threshold {integer}
set self-test-failure-threshold {integer}
set user-auth-failure-threshold {integer}
set user-auth-lockout-threshold {integer}
next
end
set status [enable|disable]
end

```

config system alarm

Parameter	Description	Type	Size	Default						
audible	Enable/disable audible alarm.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable audible alarm.</td></tr><tr><td><i>disable</i></td><td>Disable audible alarm.</td></tr></table>	Option	Description	<i>enable</i>	Enable audible alarm.	<i>disable</i>	Disable audible alarm.			
Option	Description									
<i>enable</i>	Enable audible alarm.									
<i>disable</i>	Disable audible alarm.									
status	Enable/disable alarm.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable alarm.</td></tr><tr><td><i>disable</i></td><td>Disable alarm.</td></tr></table>	Option	Description	<i>enable</i>	Enable alarm.	<i>disable</i>	Disable alarm.			
Option	Description									
<i>enable</i>	Enable alarm.									
<i>disable</i>	Disable alarm.									

config groups

Parameter	Description	Type	Size	Default
admin-auth-failure-threshold	Admin authentication failure threshold.	integer	Minimum value: 0 0 Maximum value: 1024	0
admin-auth-lockout-threshold	Admin authentication lockout threshold.	integer	Minimum value: 0 0 Maximum value: 1024	0
decryption-failure-threshold	Decryption failure threshold.	integer	Minimum value: 0 0 Maximum value: 1024	0

Parameter	Description	Type	Size	Default
encryption-failure-threshold	Encryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
fw-policy-id	Firewall policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
fw-policy-id-threshold	Firewall policy ID threshold.	integer	Minimum value: 0 Maximum value: 1024	0
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
log-full-warning-threshold	Log full warning threshold.	integer	Minimum value: 0 Maximum value: 1024	0
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295	0
replay-attempt-threshold	Replay attempt threshold.	integer	Minimum value: 0 Maximum value: 1024	0
self-test-failure-threshold	Self-test failure threshold.	integer	Minimum value: 0 Maximum value: 1	0
user-auth-failure-threshold	User authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
user-auth-lockout-threshold	User authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0

config fw-policy-violations

Parameter	Description	Type	Size	Default
dst-ip	Destination IP (0=all).	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
dst-port	Destination port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0
id	Firewall policy violations ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
src-ip	Source IP (0=all).	ipv4-address	Not Specified	0.0.0.0
src-port	Source port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0
threshold	Firewall policy violation threshold.	integer	Minimum value: 0 Maximum value: 1024	0

config system alias

Configure alias command.

```
config system alias
    Description: Configure alias command.
    edit <name>
        set command {var-string}
    next
end
```

config system alias

Parameter	Description	Type	Size	Default
command	Command list to execute.	var-string	Maximum length: 255	
name	Alias command name.	string	Maximum length: 35	

config system api-user

Configure API users.

```

config system api-user
    Description: Configure API users.
    edit <name>
        set accprofile {string}
        set api-key {password-2}
        set comments {var-string}
        set cors-allow-origin {string}
        set peer-auth [enable|disable]
        set peer-group {string}
        set schedule {string}
    config trusthost
        Description: Trusthost.
        edit <id>
            set ipv4-trusthost {ipv4-classnet}
            set ipv6-trusthost {ipv6-prefix}
            set type [ipv4-trusthost|ipv6-trusthost]
        next
    end
    set vdom <name1>, <name2>, ...
next
end

```

config system api-user

Parameter	Description	Type	Size	Default						
accprofile	Admin user access profile.	string	Maximum length: 35							
api-key	Admin user password.	password-2	Not Specified							
comments	Comment.	var-string	Maximum length: 255							
cors-allow-origin	Value for Access-Control-Allow-Origin on API responses. Avoid using '*' if possible.	string	Maximum length: 269							
name	User name.	string	Maximum length: 35							
peer-auth	Enable/disable peer authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable peer.</td></tr><tr><td><i>disable</i></td><td>Disable peer.</td></tr></table>				Option	Description	<i>enable</i>	Enable peer.	<i>disable</i>	Disable peer.
	Option	Description								
	<i>enable</i>	Enable peer.								
<i>disable</i>	Disable peer.									
peer-group	Peer group name.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
schedule	Schedule name.	string	Maximum length: 35	
vdom <name>	Virtual domains. Virtual domain name.	string	Maximum length: 79	

config trusthost

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
ipv4-trusthost	IPv4 trusted host address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ipv6-trusthost	IPv6 trusted host address.	ipv6-prefix	Not Specified	::/0
type	Trusthost type.	option	-	ipv4-trusthost

Option	Description
<i>ipv4-trusthost</i>	IPv4 trusthost.
<i>ipv6-trusthost</i>	IPv6 trusthost.

config system arp-table

Configure ARP table.

```

config system arp-table
  Description: Configure ARP table.
  edit <id>
    set interface {string}
    set ip {ipv4-address}
    set mac {mac-address}
  next
end

```

config system arp-table

Parameter	Description	Type	Size	Default
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface name.	string	Maximum length: 15	
ip	IP address.	ipv4-address	Not Specified	0.0.0.0
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00

config system automation-action

Action for automation stitches.

```
config system automation-action
  Description: Action for automation stitches.
  edit <name>
    set accprofile {string}
    set action-type [email|fortiexplorer-notification|...]
    set alicloud-access-key-id {string}
    set alicloud-access-key-secret {password}
    set alicloud-function-authorization [anonymous|function]
    set aws-api-key {password}
    set azure-api-key {password}
    set azure-function-authorization [anonymous|function|...]
    set description {var-string}
    set duration {integer}
    set email-from {var-string}
    set email-subject {var-string}
    set email-to <name1>, <name2>, ...
    set execute-security-fabric [enable|disable]
    set forticare-email [enable|disable]
    set http-body {var-string}
    config http-headers
      Description: Request headers.
      edit <id>
        set key {var-string}
        set value {var-string}
      next
    end
    set log-debug-print [enable|disable]
    set message {string}
```

```

set message-type [text|json]
set method [post|put|...]
set minimum-interval {integer}
set output-size {integer}
set port {integer}
set protocol [http|https]
set regular-expression {var-string}
set replacement-message [enable|disable]
set replacemsg-group {string}
set script {var-string}
set sdn-connector <name1>, <name2>, ...
set security-tag {string}
set system-action [reboot|shutdown|...]
set timeout {integer}
set tls-certificate {string}
set uri {var-string}
set verify-host-cert [enable|disable]
next
end

```

config system automation-action

Parameter	Description	Type	Size	Default
accprofile	Access profile for CLI script action to access FortiGate features.	string	Maximum length: 35	
action-type	Action type.	option	-	alert
	Option	Description		
	email	Send notification email.		
	fortiexplorer-notification	Send push notification to FortiExplorer.		
	alert	Generate FortiOS dashboard alert.		
	disable-ssid	Disable interface.		
	system-actions	Perform immediate system operations on this FortiGate unit.		
	quarantine	Quarantine host.		
	quarantine-forticlient	Quarantine FortiClient by EMS.		
	quarantine-nsx	Quarantine NSX instance.		
	quarantine-fortinac	Quarantine host by FortiNAC.		
	ban-ip	Ban IP address.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>aws-lambda</td><td>Send log data to integrated AWS service.</td></tr><tr><td>azure-function</td><td>Send log data to an Azure function.</td></tr><tr><td>google-cloud-function</td><td>Send log data to a Google Cloud function.</td></tr><tr><td>alicloud-function</td><td>Send log data to an AliCloud function.</td></tr><tr><td>webhook</td><td>Send an HTTP request.</td></tr><tr><td>cli-script</td><td>Run CLI script.</td></tr><tr><td>diagnose-script</td><td>Run diagnose script.</td></tr><tr><td>regular-expression</td><td>Match pattern on input text.</td></tr><tr><td>slack-notification</td><td>Send a notification message to a Slack incoming webhook.</td></tr><tr><td>microsoft-teams-notification</td><td>Send a notification message to a Microsoft Teams incoming webhook.</td></tr></table>	Option	Description	aws-lambda	Send log data to integrated AWS service.	azure-function	Send log data to an Azure function.	google-cloud-function	Send log data to a Google Cloud function.	alicloud-function	Send log data to an AliCloud function.	webhook	Send an HTTP request.	cli-script	Run CLI script.	diagnose-script	Run diagnose script.	regular-expression	Match pattern on input text.	slack-notification	Send a notification message to a Slack incoming webhook.	microsoft-teams-notification	Send a notification message to a Microsoft Teams incoming webhook.			
	Option	Description																								
	aws-lambda	Send log data to integrated AWS service.																								
	azure-function	Send log data to an Azure function.																								
	google-cloud-function	Send log data to a Google Cloud function.																								
	alicloud-function	Send log data to an AliCloud function.																								
	webhook	Send an HTTP request.																								
	cli-script	Run CLI script.																								
	diagnose-script	Run diagnose script.																								
	regular-expression	Match pattern on input text.																								
	slack-notification	Send a notification message to a Slack incoming webhook.																								
microsoft-teams-notification	Send a notification message to a Microsoft Teams incoming webhook.																									
alicloud-access-key-id	AliCloud AccessKey ID.	string	Maximum length: 35																							
alicloud-access-key-secret	AliCloud AccessKey secret.	password	Not Specified																							
alicloud-function-authorization	AliCloud function authorization type.	option	-	anonymous																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>anonymous</td><td>Anonymous authorization (No authorization required).</td></tr><tr><td>function</td><td>Function authorization (Authorization required).</td></tr></table>	Option	Description	anonymous	Anonymous authorization (No authorization required).	function	Function authorization (Authorization required).																			
	Option	Description																								
	anonymous	Anonymous authorization (No authorization required).																								
function	Function authorization (Authorization required).																									
aws-api-key	AWS API Gateway API key.	password	Not Specified																							
azure-api-key	Azure function API key.	password	Not Specified																							
azure-function-authorization	Azure function authorization level.	option	-	anonymous																						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anonymous</i></td><td>Anonymous authorization level (No authorization required).</td></tr><tr><td><i>function</i></td><td>Function authorization level (Function or Host Key required).</td></tr><tr><td><i>admin</i></td><td>Admin authorization level (Master Host Key required).</td></tr></table>	Option	Description	<i>anonymous</i>	Anonymous authorization level (No authorization required).	<i>function</i>	Function authorization level (Function or Host Key required).	<i>admin</i>	Admin authorization level (Master Host Key required).			
	Option	Description										
	<i>anonymous</i>	Anonymous authorization level (No authorization required).										
	<i>function</i>	Function authorization level (Function or Host Key required).										
<i>admin</i>	Admin authorization level (Master Host Key required).											
description	Description.	var-string	Maximum length: 255									
duration	Maximum running time for this script in seconds.	integer	Minimum value: 1 Maximum value: 36000	5								
email-from	Email sender name.	var-string	Maximum length: 127									
email-subject	Email subject.	var-string	Maximum length: 511									
email-to <name>	Email addresses. Email address.	string	Maximum length: 255									
execute-security-fabric	Enable/disable execution of CLI script on all or only one FortiGate unit in the Security Fabric.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>CLI script executes on all FortiGate units in the Security Fabric.</td></tr><tr><td><i>disable</i></td><td>CLI script executes only on the FortiGate unit that the stitch is triggered.</td></tr></table>	Option	Description	<i>enable</i>	CLI script executes on all FortiGate units in the Security Fabric.	<i>disable</i>	CLI script executes only on the FortiGate unit that the stitch is triggered.					
	Option	Description										
	<i>enable</i>	CLI script executes on all FortiGate units in the Security Fabric.										
<i>disable</i>	CLI script executes only on the FortiGate unit that the stitch is triggered.											
forticare-email	Enable/disable use of your FortiCare email address as the email-to address.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of your FortiCare email address as the email-to address.</td></tr><tr><td><i>disable</i></td><td>Disable use of your FortiCare email address as the email-to address.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of your FortiCare email address as the email-to address.	<i>disable</i>	Disable use of your FortiCare email address as the email-to address.					
	Option	Description										
	<i>enable</i>	Enable use of your FortiCare email address as the email-to address.										
<i>disable</i>	Disable use of your FortiCare email address as the email-to address.											
http-body	Request body (if necessary). Should be serialized json string.	var-string	Maximum length: 4095									
log-debug-print	Enable/disable logging debug print output from diagnose action.	option	-	disable								

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging debug print output from diagnose action.</td></tr><tr><td><i>disable</i></td><td>Disable logging debug print output from diagnose action.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging debug print output from diagnose action.	<i>disable</i>	Disable logging debug print output from diagnose action.									
	Option	Description														
	<i>enable</i>	Enable logging debug print output from diagnose action.														
<i>disable</i>	Disable logging debug print output from diagnose action.															
message	Message content.	string	Maximum length: 4095	%%log%%												
message-type	Message type.	option	-	text												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Plaintext.</td></tr><tr><td><i>json</i></td><td>Custom JSON.</td></tr></table>	Option	Description	<i>text</i>	Plaintext.	<i>json</i>	Custom JSON.									
	Option	Description														
	<i>text</i>	Plaintext.														
<i>json</i>	Custom JSON.															
method	Request method (POST, PUT, GET, PATCH or DELETE).	option	-	post												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>post</i></td><td>POST.</td></tr><tr><td><i>put</i></td><td>PUT.</td></tr><tr><td><i>get</i></td><td>GET.</td></tr><tr><td><i>patch</i></td><td>PATCH.</td></tr><tr><td><i>delete</i></td><td>DELETE.</td></tr></table>	Option	Description	<i>post</i>	POST.	<i>put</i>	PUT.	<i>get</i>	GET.	<i>patch</i>	PATCH.	<i>delete</i>	DELETE.			
	Option	Description														
	<i>post</i>	POST.														
	<i>put</i>	PUT.														
	<i>get</i>	GET.														
	<i>patch</i>	PATCH.														
<i>delete</i>	DELETE.															
minimum-interval	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000	0												
name	Name.	string	Maximum length: 64													
output-size	Number of megabytes to limit script output to (1 - 1024, default = 10).	integer	Minimum value: 1 Maximum value: 1024	10												
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0												

Parameter	Description	Type	Size	Default								
protocol	Request protocol.	option	-	http								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr></table>				Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.		
	Option	Description										
	<i>http</i>	HTTP.										
<i>https</i>	HTTPS.											
regular-expression	Regular expression string.	var-string	Maximum length: 1023									
replacement-message	Enable/disable replacement message.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable replacement message.</td></tr><tr><td><i>disable</i></td><td>Disable replacement message.</td></tr></table>				Option	Description	<i>enable</i>	Enable replacement message.	<i>disable</i>	Disable replacement message.		
	Option	Description										
	<i>enable</i>	Enable replacement message.										
<i>disable</i>	Disable replacement message.											
replacemsg-group	Replacement message group.	string	Maximum length: 35									
script	CLI script.	var-string	Maximum length: 1023									
sdn-connector <name>	NSX SDN connector names. SDN connector name.	string	Maximum length: 79									
security-tag	NSX security tag.	string	Maximum length: 255									
system-action	System action type.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reboot</i></td><td>Reboot this FortiGate unit.</td></tr><tr><td><i>shutdown</i></td><td>Shutdown this FortiGate unit.</td></tr><tr><td><i>backup-config</i></td><td>Backup current configuration to the disk revisions.</td></tr></table>				Option	Description	<i>reboot</i>	Reboot this FortiGate unit.	<i>shutdown</i>	Shutdown this FortiGate unit.	<i>backup-config</i>	Backup current configuration to the disk revisions.
	Option	Description										
	<i>reboot</i>	Reboot this FortiGate unit.										
	<i>shutdown</i>	Shutdown this FortiGate unit.										
<i>backup-config</i>	Backup current configuration to the disk revisions.											
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0								
tls-certificate	Custom TLS certificate for API request.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
uri	Request API URI.	var-string	Maximum length: 1023							
verify-host-cert	Enable/disable verification of the remote host certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of the remote host certificate.</td></tr><tr><td><i>disable</i></td><td>Disable verification of the remote host certificate.</td></tr></table>				Option	Description	<i>enable</i>	Enable verification of the remote host certificate.	<i>disable</i>	Disable verification of the remote host certificate.
Option	Description									
<i>enable</i>	Enable verification of the remote host certificate.									
<i>disable</i>	Disable verification of the remote host certificate.									

config http-headers

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
key	Request header key.	var-string	Maximum length: 1023	
value	Request header value.	var-string	Maximum length: 4095	

config system automation-condition

Condition for automation stitches.

```

config system automation-condition
  Description: Condition for automation stitches.
  edit <name>
    set condition-type [cpu|memory|...]
    set cpu-usage-percent {integer}
    set description {var-string}
    set input-id {integer}
    set input-state [open|close]
    set mem-usage-percent {integer}
    set vdom {string}
    set vpn-tunnel-name {string}
    set vpn-tunnel-state [tunnel-up|tunnel-down]
  next
end

```

config system automation-condition

Parameter	Description	Type	Size	Default								
condition-type	Condition type.	option	-	cpu								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cpu</i></td><td>CPU usage condition,</td></tr><tr><td><i>memory</i></td><td>Memory usage condition,</td></tr><tr><td><i>vpn</i></td><td>VPN state condition.</td></tr></table>	Option	Description	<i>cpu</i>	CPU usage condition,	<i>memory</i>	Memory usage condition,	<i>vpn</i>	VPN state condition.			
Option	Description											
<i>cpu</i>	CPU usage condition,											
<i>memory</i>	Memory usage condition,											
<i>vpn</i>	VPN state condition.											
cpu-usage-percent	CPU usage reaches specified percentage.	integer	Minimum value: 0 0 Maximum value: 100									
description	Description.	var-string	Maximum length: 255									
input-id *	Input ID.	integer	Minimum value: 0 0 Maximum value: 4294967295									
input-state *	Input state.	option	-	close								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Input switch is open.</td></tr><tr><td><i>close</i></td><td>Input switch is closed.</td></tr></table>	Option	Description	<i>open</i>	Input switch is open.	<i>close</i>	Input switch is closed.					
Option	Description											
<i>open</i>	Input switch is open.											
<i>close</i>	Input switch is closed.											
mem-usage-percent	Memory usage reaches specified percentage.	integer	Minimum value: 0 0 Maximum value: 100									
name	Name.	string	Maximum length: 35									
vdom	Virtual domain which the tunnel belongs to.	string	Maximum length: 31	root								
vpn-tunnel-name	VPN tunnel name.	string	Maximum length: 79									
vpn-tunnel-state	VPN tunnel state.	option	-	tunnel-up								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel-up</i></td><td>VPN tunnel is up.</td></tr><tr><td><i>tunnel-down</i></td><td>VPN tunnel is down.</td></tr></table>	Option	Description	<i>tunnel-up</i>	VPN tunnel is up.	<i>tunnel-down</i>	VPN tunnel is down.					
Option	Description											
<i>tunnel-up</i>	VPN tunnel is up.											
<i>tunnel-down</i>	VPN tunnel is down.											

* This parameter may not exist in some models.

config system automation-destination

Automation destinations.

```
config system automation-destination
  Description: Automation destinations.
  edit <name>
    set destination <name1>, <name2>, ...
    set ha-group-id {integer}
    set type [fortigate|ha-cluster]
  next
end
```

config system automation-destination

Parameter	Description	Type	Size	Default
destination <name>	Destinations. Destination.	string	Maximum length: 31	
ha-group-id	Cluster group ID set for this destination (default = 0).	integer	Minimum value: 0 Maximum value: 255	0
name	Name.	string	Maximum length: 35	
type	Destination type.	option	-	fortigate
		Option	Description	
		<i>fortigate</i>	FortiGate set as destination.	
		<i>ha-cluster</i>	HA cluster set as destination.	

config system automation-stitch

Automation stitches.

```
config system automation-stitch
  Description: Automation stitches.
  edit <name>
    config actions
      Description: Configure stitch actions.
      edit <id>
```

```

        set action {string}
        set delay {integer}
        set required [enable|disable]
    next
end
set condition <name1>, <name2>, ...
set condition-logic [and|or]
set description {var-string}
set destination <name1>, <name2>, ...
set status [enable|disable]
set trigger {string}
next
end

```

config system automation-stitch

Parameter	Description	Type	Size	Default						
condition <name>	Automation conditions. Condition name.	string	Maximum length: 79							
condition- logic	Apply AND/OR logic to the specified automation conditions.	option	-	and						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>and</i></td><td>All specified conditions must be met.</td></tr><tr><td><i>or</i></td><td>At least one specified condition needs to be met.</td></tr></table>	Option	Description	<i>and</i>	All specified conditions must be met.	<i>or</i>	At least one specified condition needs to be met.			
Option	Description									
<i>and</i>	All specified conditions must be met.									
<i>or</i>	At least one specified condition needs to be met.									
description	Description.	var-string	Maximum length: 255							
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79							
name	Name.	string	Maximum length: 35							
status	Enable/disable this stitch.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable stitch.</td></tr><tr><td><i>disable</i></td><td>Disable stitch.</td></tr></table>	Option	Description	<i>enable</i>	Enable stitch.	<i>disable</i>	Disable stitch.			
Option	Description									
<i>enable</i>	Enable stitch.									
<i>disable</i>	Disable stitch.									
trigger	Trigger name.	string	Maximum length: 35							

config actions

Parameter	Description	Type	Size	Default
action	Action name.	string	Maximum length: 64	
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600	0
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
required	Required in action chain.	option	-	disable
		Option	Description	
		enable	Required in action chain.	
		disable	Not required in action chain.	

config system automation-trigger

Trigger for automation stitches.

```
config system automation-trigger
  Description: Trigger for automation stitches.
  edit <name>
    set description {var-string}
    set event-type [ioc|event-log|...]
    set fabric-event-name {var-string}
    set fabric-event-severity {var-string}
    set faz-event-name {var-string}
    set faz-event-severity {var-string}
    set faz-event-tags {var-string}
    config fields
      Description: Customized trigger field settings.
      edit <id>
        set name {string}
        set value {var-string}
      next
    end
  set license-type [forticare-support|fortiguard-webfilter|...]
  set logid <id1>, <id2>, ...
  set report-type [posture|coverage|...]
  set serial {var-string}
  set stitch-name {string}
  set trigger-datetime {datetime}
```

```

set trigger-day {integer}
set trigger-frequency [hourly|daily|...]
set trigger-hour {integer}
set trigger-minute {integer}
set trigger-type [event-based|scheduled]
set trigger-weekday [sunday|monday|...]
set vdom <name1>, <name2>, ...
next
end

```

config system automation-trigger

Parameter	Description	Type	Size	Default																																
description	Description.	var-string	Maximum length: 255																																	
event-type	Event type.	option	-	ioc																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ioc</td><td>Indicator of compromise detected.</td></tr><tr><td>event-log</td><td>Use log ID as trigger.</td></tr><tr><td>reboot</td><td>Device reboot.</td></tr><tr><td>low-memory</td><td>Conserve mode due to low memory.</td></tr><tr><td>high-cpu</td><td>High CPU usage.</td></tr><tr><td>license-near-expiry</td><td>License near expiration date.</td></tr><tr><td>local-cert-near-expiry</td><td>The local certificate near expiration date.</td></tr><tr><td>ha-failover</td><td>HA failover.</td></tr><tr><td>config-change</td><td>Configuration change.</td></tr><tr><td>security-rating-summary</td><td>Security rating summary.</td></tr><tr><td>virus-ips-db-updated</td><td>Virus and IPS database updated.</td></tr><tr><td>faz-event</td><td>FortiAnalyzer event.</td></tr><tr><td>incoming-webhook</td><td>Incoming webhook call.</td></tr><tr><td>fabric-event</td><td>Fabric connector event.</td></tr><tr><td>ips-logs</td><td>IPS logs.</td></tr></table>	Option	Description	ioc	Indicator of compromise detected.	event-log	Use log ID as trigger.	reboot	Device reboot.	low-memory	Conserve mode due to low memory.	high-cpu	High CPU usage.	license-near-expiry	License near expiration date.	local-cert-near-expiry	The local certificate near expiration date.	ha-failover	HA failover.	config-change	Configuration change.	security-rating-summary	Security rating summary.	virus-ips-db-updated	Virus and IPS database updated.	faz-event	FortiAnalyzer event.	incoming-webhook	Incoming webhook call.	fabric-event	Fabric connector event.	ips-logs	IPS logs.			
	Option	Description																																		
	ioc	Indicator of compromise detected.																																		
	event-log	Use log ID as trigger.																																		
	reboot	Device reboot.																																		
	low-memory	Conserve mode due to low memory.																																		
	high-cpu	High CPU usage.																																		
	license-near-expiry	License near expiration date.																																		
	local-cert-near-expiry	The local certificate near expiration date.																																		
	ha-failover	HA failover.																																		
	config-change	Configuration change.																																		
	security-rating-summary	Security rating summary.																																		
	virus-ips-db-updated	Virus and IPS database updated.																																		
	faz-event	FortiAnalyzer event.																																		
	incoming-webhook	Incoming webhook call.																																		
fabric-event	Fabric connector event.																																			
ips-logs	IPS logs.																																			

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anomaly-logs</i></td><td>Anomaly logs.</td></tr><tr><td><i>virus-logs</i></td><td>Virus logs.</td></tr><tr><td><i>ssh-logs</i></td><td>SSH logs.</td></tr><tr><td><i>webfilter-violation</i></td><td>Webfilter violation.</td></tr><tr><td><i>traffic-violation</i></td><td>Traffic violation.</td></tr><tr><td><i>stitch</i></td><td>Specified stitch has been triggered.</td></tr></table>	Option	Description	<i>anomaly-logs</i>	Anomaly logs.	<i>virus-logs</i>	Virus logs.	<i>ssh-logs</i>	SSH logs.	<i>webfilter-violation</i>	Webfilter violation.	<i>traffic-violation</i>	Traffic violation.	<i>stitch</i>	Specified stitch has been triggered.							
	Option	Description																				
	<i>anomaly-logs</i>	Anomaly logs.																				
	<i>virus-logs</i>	Virus logs.																				
	<i>ssh-logs</i>	SSH logs.																				
	<i>webfilter-violation</i>	Webfilter violation.																				
	<i>traffic-violation</i>	Traffic violation.																				
<i>stitch</i>	Specified stitch has been triggered.																					
fabric-event-name	Fabric connector event handler name.	var-string	Maximum length: 255																			
fabric-event-severity	Fabric connector event severity.	var-string	Maximum length: 255																			
faz-event-name	FortiAnalyzer event handler name.	var-string	Maximum length: 255																			
faz-event-severity	FortiAnalyzer event severity.	var-string	Maximum length: 255																			
faz-event-tags	FortiAnalyzer event tags.	var-string	Maximum length: 255																			
license-type	License type.	option	-	forticare-support																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forticare-support</i></td><td>FortiCare support license.</td></tr><tr><td><i>fortiguard-webfilter</i></td><td>FortiGuard web filter license.</td></tr><tr><td><i>fortiguard-antispam</i></td><td>FortiGuard antispam license.</td></tr><tr><td><i>fortiguard-antivirus</i></td><td>FortiGuard AntiVirus license.</td></tr><tr><td><i>fortiguard-ips</i></td><td>FortiGuard IPS license.</td></tr><tr><td><i>fortiguard-management</i></td><td>FortiGuard management service license.</td></tr><tr><td><i>forticloud</i></td><td>FortiCloud license.</td></tr><tr><td><i>any</i></td><td>Any license.</td></tr></table>	Option	Description	<i>forticare-support</i>	FortiCare support license.	<i>fortiguard-webfilter</i>	FortiGuard web filter license.	<i>fortiguard-antispam</i>	FortiGuard antispam license.	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.	<i>fortiguard-ips</i>	FortiGuard IPS license.	<i>fortiguard-management</i>	FortiGuard management service license.	<i>forticloud</i>	FortiCloud license.	<i>any</i>	Any license.			
	Option	Description																				
	<i>forticare-support</i>	FortiCare support license.																				
	<i>fortiguard-webfilter</i>	FortiGuard web filter license.																				
	<i>fortiguard-antispam</i>	FortiGuard antispam license.																				
	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.																				
	<i>fortiguard-ips</i>	FortiGuard IPS license.																				
	<i>fortiguard-management</i>	FortiGuard management service license.																				
<i>forticloud</i>	FortiCloud license.																					
<i>any</i>	Any license.																					

Parameter	Description	Type	Size	Default												
logid <id>	Log IDs to trigger event. Log ID.	integer	Minimum value: 1 Maximum value: 65535													
name	Name.	string	Maximum length: 35													
report-type	Security Rating report.	option	-	posture												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>posture</i></td><td>Posture report.</td></tr><tr><td><i>coverage</i></td><td>Coverage report.</td></tr><tr><td><i>optimization</i></td><td>Optimization report</td></tr><tr><td><i>any</i></td><td>Any report.</td></tr></table>				Option	Description	<i>posture</i>	Posture report.	<i>coverage</i>	Coverage report.	<i>optimization</i>	Optimization report	<i>any</i>	Any report.		
Option	Description															
<i>posture</i>	Posture report.															
<i>coverage</i>	Coverage report.															
<i>optimization</i>	Optimization report															
<i>any</i>	Any report.															
serial	Fabric connector serial number.	var-string	Maximum length: 255													
stitch-name	Triggering stitch name.	string	Maximum length: 35													
trigger-datetime	Trigger date and time (YYYY-MM-DD HH:MM:SS).	datetime	Not Specified	0000-00-00 00:00:00												
trigger-day	Day within a month to trigger.	integer	Minimum value: 1 Maximum value: 31	1												
trigger-frequency	Scheduled trigger frequency (default = daily).	option	-	daily												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hourly</i></td><td>Run hourly.</td></tr><tr><td><i>daily</i></td><td>Run daily.</td></tr><tr><td><i>weekly</i></td><td>Run weekly.</td></tr><tr><td><i>monthly</i></td><td>Run monthly.</td></tr><tr><td><i>once</i></td><td>Run once at specified date time.</td></tr></table>				Option	Description	<i>hourly</i>	Run hourly.	<i>daily</i>	Run daily.	<i>weekly</i>	Run weekly.	<i>monthly</i>	Run monthly.	<i>once</i>	Run once at specified date time.
Option	Description															
<i>hourly</i>	Run hourly.															
<i>daily</i>	Run daily.															
<i>weekly</i>	Run weekly.															
<i>monthly</i>	Run monthly.															
<i>once</i>	Run once at specified date time.															

Parameter	Description	Type	Size	Default																
trigger-hour	Hour of the day on which to trigger (0 - 23, default = 1).	integer	Minimum value: 0 Maximum value: 23	0																
trigger-minute	Minute of the hour on which to trigger (0 - 59, default = 0).	integer	Minimum value: 0 Maximum value: 59	0																
trigger-type	Trigger type.	option	-	event-based																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event-based</i></td><td>Event based trigger.</td></tr><tr><td><i>scheduled</i></td><td>Scheduled trigger.</td></tr></table>				Option	Description	<i>event-based</i>	Event based trigger.	<i>scheduled</i>	Scheduled trigger.										
Option	Description																			
<i>event-based</i>	Event based trigger.																			
<i>scheduled</i>	Scheduled trigger.																			
trigger-weekday	Day of week for trigger.	option	-																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday.</td></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr></table>				Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.
Option	Description																			
<i>sunday</i>	Sunday.																			
<i>monday</i>	Monday.																			
<i>tuesday</i>	Tuesday.																			
<i>wednesday</i>	Wednesday.																			
<i>thursday</i>	Thursday.																			
<i>friday</i>	Friday.																			
<i>saturday</i>	Saturday.																			
vdom <name>	Virtual domain(s) that this trigger is valid for. Virtual domain name.	string	Maximum length: 79																	

config fields

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

config system autoupdate schedule

Configure update schedule.

```

config system autoupdate schedule
    Description: Configure update schedule.
    set day [Sunday|Monday|...]
    set frequency [every|daily|...]
    set status [enable|disable]
    set time {user}
end

```

config system autoupdate schedule

Parameter	Description	Type	Size	Default
day	Update day.	option	-	Monday
	Option	Description		
	<i>Sunday</i>	Update every Sunday.		
	<i>Monday</i>	Update every Monday.		
	<i>Tuesday</i>	Update every Tuesday.		
	<i>Wednesday</i>	Update every Wednesday.		
	<i>Thursday</i>	Update every Thursday.		
	<i>Friday</i>	Update every Friday.		
	<i>Saturday</i>	Update every Saturday.		
frequency	Update frequency.	option	-	automatic
	Option	Description		
	<i>every</i>	Time interval.		
	<i>daily</i>	Every day.		
	<i>weekly</i>	Every week.		
	<i>automatic</i>	Update automatically within every one hour period.		
status	Enable/disable scheduled updates.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
time	Update time.	user	Not Specified	

config system autoupdate tunneling

Configure web proxy tunneling for the FDN.

```
config system autoupdate tunneling
  Description: Configure web proxy tunneling for the FDN.
  set address {string}
  set password {password}
  set port {integer}
  set status [enable|disable]
  set username {string}
end
```

config system autoupdate tunneling

Parameter	Description	Type	Size	Default
address	Web proxy IP address or FQDN.	string	Maximum length: 63	
password	Web proxy password.	password	Not Specified	
port	Web proxy port.	integer	Minimum value: 0 Maximum value: 65535	0
status	Enable/disable web proxy tunneling.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
username	Web proxy username.	string	Maximum length: 49	

config system auto-install



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC.

Configure USB auto installation.

```
config system auto-install
  Description: Configure USB auto installation.
  set auto-install-config [enable|disable]
  set auto-install-image [enable|disable]
  set default-config-file {string}
  set default-image-file {string}
end
```

config system auto-install

Parameter	Description	Type	Size	Default						
auto-install-config	Enable/disable auto install the config in USB disk.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable config.</td></tr><tr><td><i>disable</i></td><td>Disable config.</td></tr></table>	Option	Description	<i>enable</i>	Enable config.	<i>disable</i>	Disable config.			
Option	Description									
<i>enable</i>	Enable config.									
<i>disable</i>	Disable config.									

Parameter	Description	Type	Size	Default						
auto-install-image	Enable/disable auto install the image in USB disk.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable config.</td></tr><tr><td><i>disable</i></td><td>Disable config.</td></tr></table>				Option	Description	<i>enable</i>	Enable config.	<i>disable</i>	Disable config.
	Option	Description								
	<i>enable</i>	Enable config.								
<i>disable</i>	Disable config.									
default-config-file	Default config file name in USB disk.	string	Maximum length: 127	fgt_system.conf						
default-image-file	Default image file name in USB disk.	string	Maximum length: 127	image.out						

config system auto-scale



This command is available for model(s): FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure system auto-scaling.

```
config system auto-scale
  Description: Configure system auto-scaling.
  set callback-url {var-string}
  set cloud-mode {string}
  set hb-interval {integer}
```

```

set primary-ip {ipv4-address-any}
set psksecret {password-3}
set role [primary|secondary]
set status [enable|disable]
set sync-interface {string}
end

```

config system auto-scale

Parameter	Description	Type	Size	Default						
callback-url	Callback URL.	var-string	Maximum length: 4095							
cloud-mode	Auto-scaling cloud mode.	string	Maximum length: 31							
hb-interval	Time between sending heartbeat packets (5 - 120 seconds). Increase to reduce false positives.	integer	Minimum value: 5 Maximum value: 120	10						
primary-ip	Primary IP address.	ipv4-address-any	Not Specified	0.0.0.0						
psksecret	Pre-shared secret for auto-scaling authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified							
role	Auto-scaling role.	option	-	secondary						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>primary</i></td><td>Primary in auto-scaling.</td></tr><tr><td><i>secondary</i></td><td>Secondary in auto-scaling.</td></tr></table>	Option	Description	<i>primary</i>	Primary in auto-scaling.	<i>secondary</i>	Secondary in auto-scaling.			
Option	Description									
<i>primary</i>	Primary in auto-scaling.									
<i>secondary</i>	Secondary in auto-scaling.									
status	Auto-Scaling status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable system auto-scaling</td></tr><tr><td><i>disable</i></td><td>Disable system auto-scaling.</td></tr></table>	Option	Description	<i>enable</i>	Enable system auto-scaling	<i>disable</i>	Disable system auto-scaling.			
Option	Description									
<i>enable</i>	Enable system auto-scaling									
<i>disable</i>	Disable system auto-scaling.									
sync-interface	Interface used for synchronization.	string	Maximum length: 15							

config system auto-script

Configure auto script.


```

config system auto-script
  Description: Configure auto script.
  edit <name>
    set interval {integer}
    set output-size {integer}
    set repeat {integer}
    set script {var-string}
    set start [manual|auto]
    set timeout {integer}
  next
end

```

config system auto-script

Parameter	Description	Type	Size	Default						
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600	0						
name	Auto script name.	string	Maximum length: 35							
output-size	Number of megabytes to limit script output to (10 - 1024, default = 10).	integer	Minimum value: 10 Maximum value: 1024	10						
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535	1						
script	List of FortiOS CLI commands to repeat.	var-string	Maximum length: 1023							
start	Script starting mode.	option	-	manual						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>manual</i></td><td>Starting manually.</td></tr><tr><td><i>auto</i></td><td>Starting automatically.</td></tr></table>				Option	Description	<i>manual</i>	Starting manually.	<i>auto</i>	Starting automatically.
	Option	Description								
	<i>manual</i>	Starting manually.								
<i>auto</i>	Starting automatically.									
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0						

config system bypass



This command is available for model(s): FortiGate 2500E, FortiGate 400E Bypass, FortiGate 800D, FortiGate 80F Bypass, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure system bypass.

```
config system bypass
  Description: Configure system bypass.
  set auto-recover [enable|disable]
  set bypass-timeout [2|4|...]
  set bypass-watchdog [enable|disable]
  set poweroff-bypass [enable|disable]
end
```

config system bypass

Parameter	Description	Type	Size	Default				
auto-recover *	Automatically recover from bypass mode after system reboot.	option	-	enable				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Recover interfaces from bypass mode. The actual mode is determined by poweron-bypass setting.</td></tr></table>	Option	Description	enable	Recover interfaces from bypass mode. The actual mode is determined by poweron-bypass setting.			
Option	Description							
enable	Recover interfaces from bypass mode. The actual mode is determined by poweron-bypass setting.							

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Keep interfaces in bypass mode if bypass was previously triggered.		
bypass-timeout *	timeout setting for bypass watchdog	option	-	10
	Option	Description		
	2	2 second		
	4	4 second		
	6	6 second		
	8	8 second		
	10	10 second		
	12	12 second		
	14	14 second		
bypass-watchdog	watchdog to bypass interfaces in case of software/hardware failure	option	-	disable
	Option	Description		
	<i>enable</i>	Enable watchdog for bypass interfaces.		
	<i>disable</i>	Disable watchdog for bypass interfaces.		
poweroff-bypass *	set interface bypass state in power off	option	-	disable
	Option	Description		
	<i>enable</i>	Enable bypass when power off.		
	<i>disable</i>	Disable bypass when power off.		

* This parameter may not exist in some models.

config system central-management

Configure central management.

```
config system central-management
  Description: Configure central management.
  set allow-monitor [enable|disable]
  set allow-push-configuration [enable|disable]
  set allow-push-firmware [enable|disable]
```

```

set allow-remote-firmware-upgrade [enable|disable]
set allow-remote-lte-firmware-upgrade [enable|disable]
set ca-cert {user}
set enc-algorithm [default|high|...]
set fmg {user}
set fmg-source-ip {ipv4-address}
set fmg-source-ip6 {ipv6-address}
set fmg-update-http-header [enable|disable]
set fmg-update-port [8890|443]
set fortigate-cloud-sso-default-profile {string}
set include-default-servers [enable|disable]
set interface {string}
set interface-select-method [auto|sdwan|...]
set local-cert {string}
set ltefw-upgrade-frequency [everyHour|every12hour|...]
set ltefw-upgrade-time {string}
set mode [normal|backup]
set schedule-config-restore [enable|disable]
set schedule-script-restore [enable|disable]
set serial-number {user}
config server-list
    Description: Additional servers that the FortiGate can use for updates (for AV, IPS,
updates) and ratings (for web filter and antispam ratings) servers.
    edit <id>
        set addr-type [ipv4|ipv6|...]
        set fqdn {string}
        set server-address {ipv4-address}
        set server-address6 {ipv6-address}
        set server-type {option1}, {option2}, ...
    next
end
set type [fortimanager|fortiguard|...]
set use-elbc-vdom [enable|disable]
set vdom {string}
set vrf-select {integer}
end

```

config system central-management

Parameter	Description	Type	Size	Default						
allow-monitor	Enable/disable allowing the central management server to remotely monitor this FortiGate unit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable remote monitoring of device.</td></tr><tr><td><i>disable</i></td><td>Disable remote monitoring of device.</td></tr></table>				Option	Description	<i>enable</i>	Enable remote monitoring of device.	<i>disable</i>	Disable remote monitoring of device.
Option	Description									
<i>enable</i>	Enable remote monitoring of device.									
<i>disable</i>	Disable remote monitoring of device.									

Parameter	Description	Type	Size	Default								
allow-push-configuration	Enable/disable allowing the central management server to push configuration changes to this FortiGate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable push configuration.</td></tr><tr><td><i>disable</i></td><td>Disable push configuration.</td></tr></table>	Option	Description	<i>enable</i>	Enable push configuration.	<i>disable</i>	Disable push configuration.					
Option	Description											
<i>enable</i>	Enable push configuration.											
<i>disable</i>	Disable push configuration.											
allow-push-firmware	Enable/disable allowing the central management server to push firmware updates to this FortiGate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable push firmware.</td></tr><tr><td><i>disable</i></td><td>Disable push firmware.</td></tr></table>	Option	Description	<i>enable</i>	Enable push firmware.	<i>disable</i>	Disable push firmware.					
Option	Description											
<i>enable</i>	Enable push firmware.											
<i>disable</i>	Disable push firmware.											
allow-remote-firmware-upgrade	Enable/disable remotely upgrading the firmware on this FortiGate from the central management server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable remote firmware upgrade.</td></tr><tr><td><i>disable</i></td><td>Disable remote firmware upgrade.</td></tr></table>	Option	Description	<i>enable</i>	Enable remote firmware upgrade.	<i>disable</i>	Disable remote firmware upgrade.					
Option	Description											
<i>enable</i>	Enable remote firmware upgrade.											
<i>disable</i>	Disable remote firmware upgrade.											
allow-remote-lte-firmware-upgrade *	Enable/disable remotely upgrading the lte firmware on this FortiGate from the central management server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable remote lte firmware upgrade.</td></tr><tr><td><i>disable</i></td><td>Disable remote lte firmware upgrade.</td></tr></table>	Option	Description	<i>enable</i>	Enable remote lte firmware upgrade.	<i>disable</i>	Disable remote lte firmware upgrade.					
Option	Description											
<i>enable</i>	Enable remote lte firmware upgrade.											
<i>disable</i>	Disable remote lte firmware upgrade.											
ca-cert	CA certificate to be used by FGFM protocol.	user	Not Specified									
enc-algorithm	Encryption strength for communications between the FortiGate and central management.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>High strength algorithms and medium-strength 128-bit key length algorithms.</td></tr><tr><td><i>high</i></td><td>128-bit and larger key length algorithms.</td></tr><tr><td><i>low</i></td><td>64-bit or 56-bit key length algorithms without export restrictions.</td></tr></table>	Option	Description	<i>default</i>	High strength algorithms and medium-strength 128-bit key length algorithms.	<i>high</i>	128-bit and larger key length algorithms.	<i>low</i>	64-bit or 56-bit key length algorithms without export restrictions.			
Option	Description											
<i>default</i>	High strength algorithms and medium-strength 128-bit key length algorithms.											
<i>high</i>	128-bit and larger key length algorithms.											
<i>low</i>	64-bit or 56-bit key length algorithms without export restrictions.											

Parameter	Description	Type	Size	Default						
fmg	IP address or FQDN of the FortiManager.	user	Not Specified							
fmg-source-ip	IPv4 source address that this FortiGate uses when communicating with FortiManager.	ipv4-address	Not Specified	0.0.0.0						
fmg-source-ip6	IPv6 source address that this FortiGate uses when communicating with FortiManager.	ipv6-address	Not Specified	::						
fmg-update-http-header	Enable/disable inclusion of HTTP header in update request.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable inclusion of HTTP header in update request.</td></tr><tr><td>disable</td><td>Disable inclusion of HTTP header in update request.</td></tr></table>	Option	Description	enable	Enable inclusion of HTTP header in update request.	disable	Disable inclusion of HTTP header in update request.			
Option	Description									
enable	Enable inclusion of HTTP header in update request.									
disable	Disable inclusion of HTTP header in update request.									
fmg-update-port	Port used to communicate with FortiManager that is acting as a FortiGuard update server.	option	-	8890						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>8890</td><td>Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.</td></tr><tr><td>443</td><td>Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.</td></tr></table>	Option	Description	8890	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.	443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.			
Option	Description									
8890	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.									
443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.									
fortigate-cloud-sso-default-profile	Override access profile.	string	Maximum length: 35							
include-default-servers	Enable/disable inclusion of public FortiGuard servers in the override server list.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable inclusion of public FortiGuard servers in the override server list.</td></tr><tr><td>disable</td><td>Disable inclusion of public FortiGuard servers in the override server list.</td></tr></table>	Option	Description	enable	Enable inclusion of public FortiGuard servers in the override server list.	disable	Disable inclusion of public FortiGuard servers in the override server list.			
Option	Description									
enable	Enable inclusion of public FortiGuard servers in the override server list.									
disable	Disable inclusion of public FortiGuard servers in the override server list.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.					
Option	Description									
auto	Set outgoing interface automatically.									

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
	Option	Description												
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.												
<i>specify</i>	Set outgoing interface manually.													
local-cert	Certificate to be used by FGFM protocol.	string	Maximum length: 35											
ltefw-upgrade-frequency *	Set LTE firmware auto pushdown frequency.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>everyHour</i></td><td>Auto check and pushdown LTE firmware every hour</td></tr><tr><td><i>every12hour</i></td><td>Auto check and pushdown LTE firmware every 12 hours</td></tr><tr><td><i>everyDay</i></td><td>Auto check and pushdown LTE firmware every day</td></tr><tr><td><i>everyWeek</i></td><td>Auto check and pushdown LTE firmware every week</td></tr></table>	Option	Description	<i>everyHour</i>	Auto check and pushdown LTE firmware every hour	<i>every12hour</i>	Auto check and pushdown LTE firmware every 12 hours	<i>everyDay</i>	Auto check and pushdown LTE firmware every day	<i>everyWeek</i>	Auto check and pushdown LTE firmware every week			
	Option	Description												
	<i>everyHour</i>	Auto check and pushdown LTE firmware every hour												
	<i>every12hour</i>	Auto check and pushdown LTE firmware every 12 hours												
	<i>everyDay</i>	Auto check and pushdown LTE firmware every day												
<i>everyWeek</i>	Auto check and pushdown LTE firmware every week													
ltefw-upgrade-time *	Schedule next LTE firmware upgrade time (Local Time). Format: YYYY-MM-DD HH:MM:SS	string	Maximum length: 35											
mode	Central management mode.	option	-	normal										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Manage and configure this FortiGate from FortiManager.</td></tr><tr><td><i>backup</i></td><td>Manage and configure this FortiGate locally and back up its configuration to FortiManager.</td></tr></table>	Option	Description	<i>normal</i>	Manage and configure this FortiGate from FortiManager.	<i>backup</i>	Manage and configure this FortiGate locally and back up its configuration to FortiManager.							
	Option	Description												
	<i>normal</i>	Manage and configure this FortiGate from FortiManager.												
<i>backup</i>	Manage and configure this FortiGate locally and back up its configuration to FortiManager.													
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiGate.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable scheduled configuration restore.</td></tr><tr><td><i>disable</i></td><td>Disable scheduled configuration restore.</td></tr></table>	Option	Description	<i>enable</i>	Enable scheduled configuration restore.	<i>disable</i>	Disable scheduled configuration restore.							
	Option	Description												
	<i>enable</i>	Enable scheduled configuration restore.												
<i>disable</i>	Disable scheduled configuration restore.													
schedule-script-restore	Enable/disable allowing the central management server to restore the scripts stored on this FortiGate.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable scheduled script restore.</td></tr><tr><td><i>disable</i></td><td>Disable scheduled script restore.</td></tr></table>	Option	Description	<i>enable</i>	Enable scheduled script restore.	<i>disable</i>	Disable scheduled script restore.							
	Option	Description												
	<i>enable</i>	Enable scheduled script restore.												
<i>disable</i>	Disable scheduled script restore.													

Parameter	Description	Type	Size	Default								
serial-number	Serial number.	user	Not Specified									
type	Central management type.	option	-	none **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fortimanager</td><td>FortiManager.</td></tr><tr><td>fortiguard</td><td>Central management of this FortiGate using FortiCloud.</td></tr><tr><td>none</td><td>No central management.</td></tr></table>				Option	Description	fortimanager	FortiManager.	fortiguard	Central management of this FortiGate using FortiCloud.	none	No central management.
Option	Description											
fortimanager	FortiManager.											
fortiguard	Central management of this FortiGate using FortiCloud.											
none	No central management.											
use-elbc-vdom *	Enable/disable use of special ELBC config sync VDOM to connect to FortiManager.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>enable</td></tr><tr><td>disable</td><td>disable</td></tr></table>				Option	Description	enable	enable	disable	disable		
Option	Description											
enable	enable											
disable	disable											
vdom	Virtual domain (VDOM) name to use when communicating with FortiManager.	string	Maximum length: 31	root								
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0								

* This parameter may not exist in some models.

** Values may differ between models.

config server-list

Parameter	Description	Type	Size	Default								
addr-type	Indicate whether the FortiGate communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.	option	-	ipv4								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 address.</td></tr><tr><td>ipv6</td><td>IPv6 address.</td></tr><tr><td>fqdn</td><td>FQDN.</td></tr></table>				Option	Description	ipv4	IPv4 address.	ipv6	IPv6 address.	fqdn	FQDN.
	Option	Description										
	ipv4	IPv4 address.										
	ipv6	IPv6 address.										
fqdn	FQDN.											
fqdn	FQDN address of override server.	string	Maximum length: 255									

Parameter	Description	Type	Size	Default										
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
server-address	IPv4 address of override server.	ipv4-address	Not Specified	0.0.0.0										
server-address6	IPv6 address of override server.	ipv6-address	Not Specified	::										
server-type	FortiGuard service type.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>update</td><td>AV, IPS, and AV-query update server.</td></tr><tr><td>rating</td><td>Web filter and anti-spam rating server.</td></tr><tr><td>vpatch-query</td><td>Virtual patch query server.</td></tr><tr><td>iot-collect</td><td>IoT device collection server.</td></tr></table>				Option	Description	update	AV, IPS, and AV-query update server.	rating	Web filter and anti-spam rating server.	vpatch-query	Virtual patch query server.	iot-collect	IoT device collection server.
Option	Description													
update	AV, IPS, and AV-query update server.													
rating	Web filter and anti-spam rating server.													
vpatch-query	Virtual patch query server.													
iot-collect	IoT device collection server.													

config system cloud-service

Configure system cloud service.

```
config system cloud-service
  Description: Configure system cloud service.
  edit <name>
    set gck-access-token-lifetime {integer}
    set gck-keyid {string}
    set gck-private-key {string}
    set gck-service-account {string}
    set traffic-vdom {string}
    set vendor [unknown|google-cloud-kms]
  next
end
```

config system cloud-service

Parameter	Description	Type	Size	Default
gck-access-token-lifetime	Lifetime of automatically generated access tokens in minutes (default is 60 minutes).	integer	Minimum value: 1 Maximum value: 3600	60

Parameter	Description	Type	Size	Default						
gck-keyid	Key id, also referred as "kid".	string	Maximum length: 127							
gck-private-key	Service account private key in PEM format (e.g. "---BEGIN PRIVATE KEY-----\ ...").	string	Maximum length: 8191							
gck-service-account	Service account (e.g. "account-id@sampledomain.com").	string	Maximum length: 285							
name	Name.	string	Maximum length: 35							
traffic-vdom	Vdom used to communicate with cloud service.	string	Maximum length: 31							
vendor	Cloud service vendor.	option	-	unknown						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>unknown</td><td>Unknown type of cloud service vendor.</td></tr><tr><td>google-cloud-kms</td><td>Google Cloud KMS service.</td></tr></table>				Option	Description	unknown	Unknown type of cloud service vendor.	google-cloud-kms	Google Cloud KMS service.
Option	Description									
unknown	Unknown type of cloud service vendor.									
google-cloud-kms	Google Cloud KMS service.									

config system console

Configure console.

```
config system console
  Description: Configure console.
  set fortiexplorer [enable|disable]
  set login [enable|disable]
  set output [standard|more]
end
```

config system console

Parameter	Description	Type	Size	Default
fortiexplorer *	Enable/disable access for FortiExplorer.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiExplorer access.		
	<i>disable</i>	Disable FortiExplorer access.		
login	Enable/disable serial console and FortiExplorer.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Console login enable.		
	<i>disable</i>	Console login disable.		
output	Console output mode.	option	-	more
	Option	Description		
	<i>standard</i>	Standard output.		
	<i>more</i>	More page output.		

* This parameter may not exist in some models.

config system csf

Add this FortiGate to a Security Fabric or set up a new Security Fabric on this FortiGate.

```
config system csf
    Description: Add this FortiGate to a Security Fabric or set up a new Security Fabric on this
    FortiGate.
    set accept-auth-by-cert [disable|enable]
    set authorization-request-type [serial|certificate]
    set certificate {string}
    set configuration-sync [default|local]
    set downstream-access [enable|disable]
    set downstream-accprofile {string}
    config fabric-connector
        Description: Fabric connector configuration.
        edit <serial>
            set accprofile {string}
            set configuration-write-access [enable|disable]
            set vdom <name1>, <name2>, ...
        next
    end
    set fabric-object-unification [default|local]
    set fabric-workers {integer}
    set file-mgmt [enable|disable]
    set file-quota {integer}
    set file-quota-warning {integer}
    set forticloud-account-enforcement [enable|disable]
    set group-name {string}
    set group-password {password}
    set legacy-authentication [disable|enable]
    set log-unification [disable|enable]
    set saml-configuration-sync [default|local]
    set source-ip {ipv4-address}
```

```

set status [enable|disable]
config trusted-list
  Description: Pre-authorized and blocked security fabric nodes.
  edit <name>
    set action [accept|deny]
    set authorization-type [serial|certificate]
    set certificate {var-string}
    set downstream-authorization [enable|disable]
    set ha-members {string}
    set index {integer}
    set serial {string}
  next
end
set uid {string}
set upstream {string}
set upstream-interface {string}
set upstream-interface-select-method [auto|sdwan|...]
set upstream-port {integer}
end

```

config system csf

Parameter	Description	Type	Size	Default						
accept-auth-by-cert	Accept connections with unknown certificates and ask admin for approval.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not accept SSL connections with unknown certificates.</td></tr><tr><td>enable</td><td>Accept SSL connections without automatic certificate verification.</td></tr></table>				Option	Description	disable	Do not accept SSL connections with unknown certificates.	enable	Accept SSL connections without automatic certificate verification.
Option	Description									
disable	Do not accept SSL connections with unknown certificates.									
enable	Accept SSL connections without automatic certificate verification.									
authorization-request-type	Authorization request type.	option	-	serial						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>serial</td><td>Request verification by serial number.</td></tr><tr><td>certificate</td><td>Request verification by certificate.</td></tr></table>				Option	Description	serial	Request verification by serial number.	certificate	Request verification by certificate.
Option	Description									
serial	Request verification by serial number.									
certificate	Request verification by certificate.									
certificate	Certificate.	string	Maximum length: 35							
configuration-sync	Configuration sync mode.	option	-	default						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.</td></tr><tr><td>local</td><td>Do not synchronize configuration with root node.</td></tr></table>	Option	Description	default	Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.	local	Do not synchronize configuration with root node.			
	Option	Description								
	default	Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.								
local	Do not synchronize configuration with root node.									
downstream-access	Enable/disable downstream device access to this device's configuration and data.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable downstream device access to this device's configuration and data.</td></tr><tr><td>disable</td><td>Disable downstream device access to this device's configuration and data.</td></tr></table>	Option	Description	enable	Enable downstream device access to this device's configuration and data.	disable	Disable downstream device access to this device's configuration and data.			
	Option	Description								
	enable	Enable downstream device access to this device's configuration and data.								
disable	Disable downstream device access to this device's configuration and data.									
downstream-accprofile	Default access profile for requests from downstream devices.	string	Maximum length: 35							
fabric-object-unification	Fabric CMDB Object Unification.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Global CMDB objects will be synchronized in Security Fabric.</td></tr><tr><td>local</td><td>Global CMDB objects will not be synchronized to and from this device.</td></tr></table>	Option	Description	default	Global CMDB objects will be synchronized in Security Fabric.	local	Global CMDB objects will not be synchronized to and from this device.			
	Option	Description								
	default	Global CMDB objects will be synchronized in Security Fabric.								
local	Global CMDB objects will not be synchronized to and from this device.									
fabric-workers	Number of worker processes for Security Fabric daemon.	integer	Minimum value: 2 1 Maximum value: 4							
file-mgmt	Enable/disable Security Fabric daemon file management.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable daemon file management.</td></tr><tr><td>disable</td><td>Disable daemon file management.</td></tr></table>	Option	Description	enable	Enable daemon file management.	disable	Disable daemon file management.			
	Option	Description								
	enable	Enable daemon file management.								
disable	Disable daemon file management.									
file-quota	Maximum amount of memory that can be used by the daemon files (in bytes).	integer	Minimum value: 0 0 Maximum value: 4294967295							
file-quota-warning	Warn when the set percentage of quota has been used.	integer	Minimum value: 90 1 Maximum value: 99							

Parameter	Description	Type	Size	Default						
forticloud-account-enforcement	Fabric FortiCloud account unification.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiCloud account ID matching for Security Fabric.</td></tr><tr><td><i>disable</i></td><td>Disable FortiCloud account ID matching for Security Fabric.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCloud account ID matching for Security Fabric.	<i>disable</i>	Disable FortiCloud account ID matching for Security Fabric.			
Option	Description									
<i>enable</i>	Enable FortiCloud account ID matching for Security Fabric.									
<i>disable</i>	Disable FortiCloud account ID matching for Security Fabric.									
group-name	Security Fabric group name. All FortiGates in a Security Fabric must have the same group name.	string	Maximum length: 35							
group-password	Security Fabric group password. For legacy authentication, fabric members must have the same group password.	password	Not Specified							
legacy-authentication	Enable/disable legacy authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not accept legacy authentication requests.</td></tr><tr><td><i>enable</i></td><td>Accept legacy authentication requests.</td></tr></table>	Option	Description	<i>disable</i>	Do not accept legacy authentication requests.	<i>enable</i>	Accept legacy authentication requests.			
Option	Description									
<i>disable</i>	Do not accept legacy authentication requests.									
<i>enable</i>	Accept legacy authentication requests.									
log-unification	Enable/disable broadcast of discovery messages for log unification.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable broadcast of discovery messages for log unification.</td></tr><tr><td><i>enable</i></td><td>Enable broadcast of discovery messages for log unification.</td></tr></table>	Option	Description	<i>disable</i>	Disable broadcast of discovery messages for log unification.	<i>enable</i>	Enable broadcast of discovery messages for log unification.			
Option	Description									
<i>disable</i>	Disable broadcast of discovery messages for log unification.									
<i>enable</i>	Enable broadcast of discovery messages for log unification.									
saml-configuration-sync	SAML setting configuration synchronization.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>SAML setting for fabric members is created by fabric root.</td></tr><tr><td><i>local</i></td><td>Do not apply SAML configuration generated by root.</td></tr></table>	Option	Description	<i>default</i>	SAML setting for fabric members is created by fabric root.	<i>local</i>	Do not apply SAML configuration generated by root.			
Option	Description									
<i>default</i>	SAML setting for fabric members is created by fabric root.									
<i>local</i>	Do not apply SAML configuration generated by root.									
source-ip	Source IP address for communication with the upstream FortiGate.	ipv4-address	Not Specified	0.0.0.0						
status	Enable/disable Security Fabric.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Security Fabric.		
	<i>disable</i>	Disable Security Fabric.		
uid	Unique ID of the current CSF node	string	Maximum length: 35	
upstream	IP/FQDN of the FortiGate upstream from this FortiGate in the Security Fabric.	string	Maximum length: 255	
upstream-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
upstream-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
upstream-port	The port number to use to communicate with the FortiGate upstream from this FortiGate in the Security Fabric (default = 8013).	integer	Minimum value: 8013 1 Maximum value: 65535	

config fabric-connector

Parameter	Description	Type	Size	Default						
accprofile	Override access profile.	string	Maximum length: 35							
configuration-write-access	Enable/disable downstream device write access to configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable downstream device write access to configuration.</td></tr><tr><td><i>disable</i></td><td>Disable downstream device write access to configuration.</td></tr></table>				Option	Description	<i>enable</i>	Enable downstream device write access to configuration.	<i>disable</i>	Disable downstream device write access to configuration.
Option	Description									
<i>enable</i>	Enable downstream device write access to configuration.									
<i>disable</i>	Disable downstream device write access to configuration.									
serial	Serial.	string	Maximum length: 19							

Parameter	Description	Type	Size	Default
vdom <name>	Virtual domains that the connector has access to. If none are set, the connector will only have access to the VDOM that it joins the Security Fabric through. Virtual domain name.	string	Maximum length: 79	

config trusted-list

Parameter	Description	Type	Size	Default						
action	Security fabric authorization action.	option	-	accept						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept authorization request.</td></tr><tr><td><i>deny</i></td><td>Deny authorization request.</td></tr></table>	Option	Description	<i>accept</i>	Accept authorization request.	<i>deny</i>	Deny authorization request.			
Option	Description									
<i>accept</i>	Accept authorization request.									
<i>deny</i>	Deny authorization request.									
authorization-type	Authorization type.	option	-	serial						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>serial</i></td><td>Verify downstream by serial number.</td></tr><tr><td><i>certificate</i></td><td>Verify downstream by certificate.</td></tr></table>	Option	Description	<i>serial</i>	Verify downstream by serial number.	<i>certificate</i>	Verify downstream by certificate.			
Option	Description									
<i>serial</i>	Verify downstream by serial number.									
<i>certificate</i>	Verify downstream by certificate.									
certificate	Certificate.	var-string	Maximum length: 32767							
downstream-authorization	Trust authorizations by this node's administrator.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable downstream authorization.</td></tr><tr><td><i>disable</i></td><td>Disable downstream authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable downstream authorization.	<i>disable</i>	Disable downstream authorization.			
Option	Description									
<i>enable</i>	Enable downstream authorization.									
<i>disable</i>	Disable downstream authorization.									
ha-members	HA members.	string	Maximum length: 19							
index	Index of the downstream in tree.	integer	Minimum value: 1 Maximum value: 1024	0						
name	Name.	string	Maximum length: 35							
serial	Serial.	string	Maximum length: 19							

config system custom-language

Configure custom languages.

```
config system custom-language
  Description: Configure custom languages.
  edit <name>
    set comments {var-string}
    set filename {string}
  next
end
```

config system custom-language

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
filename	Custom language file path.	string	Maximum length: 63	
name	Name.	string	Maximum length: 35	

config system ddns

Configure DDNS.

```
config system ddns
  Description: Configure DDNS.
  edit <ddnsid>
    set addr-type [ipv4|ipv6]
    set bound-ip {string}
    set clear-text [disable|enable]
    set ddns-auth [disable|tsig]
    set ddns-domain {string}
    set ddns-key {password_aes256}
    set ddns-keyname {string}
    set ddns-password {password}
    set ddns-server [dyndns.org|dyns.net|...]
    set ddns-server-addr <addr1>, <addr2>, ...
    set ddns-sn {string}
    set ddns-ttl {integer}
    set ddns-username {string}
    set ddns-zone {string}
    set monitor-interface <interface-name1>, <interface-name2>, ...
    set server-type [ipv4|ipv6]
```

```

    set ssl-certificate {string}
    set update-interval {integer}
    set use-public-ip [disable|enable]
next
end

```

config system ddns

Parameter	Description	Type	Size	Default
addr-type	Address type of interface address in DDNS update.	option	-	ipv4
	Option		Description	
	ipv4		Use IPv4 address of the interface.	
	ipv6		Use IPv6 address of the interface.	
bound-ip	Bound IP address. Read-only.	string	Maximum length: 46	
clear-text	Enable/disable use of clear text connections.	option	-	disable
	Option		Description	
	disable		Disable use of clear text connections.	
	enable		Enable use of clear text connections.	
ddns-auth	Enable/disable TSIG authentication for your DDNS server.	option	-	disable
	Option		Description	
	disable		Disable DDNS authentication.	
	tsig		Enable TSIG authentication based on RFC2845.	
ddns-domain	Your fully qualified domain name. For example, yourname.ddns.com.	string	Maximum length: 64	
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified	
ddns-keyname	DDNS update key name.	string	Maximum length: 64	
ddns-password	DDNS password.	password	Not Specified	
ddns-server	Select a DDNS service provider.	option	-	

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dyndns.org</i></td><td>members.dyndns.org and dnsalias.com</td></tr><tr><td><i>dyns.net</i></td><td>www.dyns.net</td></tr><tr><td><i>tzo.com</i></td><td>rh.tzo.com</td></tr><tr><td><i>vavic.com</i></td><td>Peanut Hull</td></tr><tr><td><i>dipdns.net</i></td><td>dipdnsserver.dipdns.com</td></tr><tr><td><i>now.net.cn</i></td><td>ip.todayisp.com</td></tr><tr><td><i>dhs.org</i></td><td>members.dhs.org</td></tr><tr><td><i>easydns.com</i></td><td>members.easydns.com</td></tr><tr><td><i>genericDDNS</i></td><td>Generic DDNS based on RFC2136.</td></tr><tr><td><i>FortiGuardDDNS</i></td><td>FortiGuard DDNS service.</td></tr><tr><td><i>noip.com</i></td><td>dynupdate.no-ip.com</td></tr></table>	Option	Description	<i>dyndns.org</i>	members.dyndns.org and dnsalias.com	<i>dyns.net</i>	www.dyns.net	<i>tzo.com</i>	rh.tzo.com	<i>vavic.com</i>	Peanut Hull	<i>dipdns.net</i>	dipdnsserver.dipdns.com	<i>now.net.cn</i>	ip.todayisp.com	<i>dhs.org</i>	members.dhs.org	<i>easydns.com</i>	members.easydns.com	<i>genericDDNS</i>	Generic DDNS based on RFC2136.	<i>FortiGuardDDNS</i>	FortiGuard DDNS service.	<i>noip.com</i>	dynupdate.no-ip.com			
	Option	Description																										
	<i>dyndns.org</i>	members.dyndns.org and dnsalias.com																										
	<i>dyns.net</i>	www.dyns.net																										
	<i>tzo.com</i>	rh.tzo.com																										
	<i>vavic.com</i>	Peanut Hull																										
	<i>dipdns.net</i>	dipdnsserver.dipdns.com																										
	<i>now.net.cn</i>	ip.todayisp.com																										
	<i>dhs.org</i>	members.dhs.org																										
	<i>easydns.com</i>	members.easydns.com																										
	<i>genericDDNS</i>	Generic DDNS based on RFC2136.																										
	<i>FortiGuardDDNS</i>	FortiGuard DDNS service.																										
<i>noip.com</i>	dynupdate.no-ip.com																											
ddns-server-addr <addr>	Generic DDNS server IP/FQDN list. IP address or FQDN of the server.	string	Maximum length: 256																									
ddns-sn	DDNS Serial Number.	string	Maximum length: 64																									
ddns-ttl	Time-to-live for DDNS packets.	integer	Minimum value: 300 60 Maximum value: 86400																									
ddns-username	DDNS user name.	string	Maximum length: 64																									
ddns-zone	Zone of your domain name (for example, DDNS.com).	string	Maximum length: 64																									
ddnsid	DDNS ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																									
monitor-interface <interface-name>	Monitored interface. Interface name.	string	Maximum length: 79																									
server-type	Address type of the DDNS server.	option	-	ipv4																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>Use IPv4 addressing.</td></tr></table>	Option	Description	<i>ipv4</i>	Use IPv4 addressing.																							
	Option	Description																										
<i>ipv4</i>	Use IPv4 addressing.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ipv6</i>	Use IPv6 addressing.		
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
update-interval	DDNS update interval (60 - 2592000 sec, 0 means default).	integer	Minimum value: 60 Maximum value: 2592000	0
use-public-ip	Enable/disable use of public IP address.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of public IP address.		
	<i>enable</i>	Enable use of public IP address.		

config system dedicated-mgmt

Configure dedicated management.

```

config system dedicated-mgmt
    Description: Configure dedicated management.
    set default-gateway {ipv4-address}
    set dhcp-end-ip {ipv4-address}
    set dhcp-netmask {ipv4-netmask}
    set dhcp-server [enable|disable]
    set dhcp-start-ip {ipv4-address}
    set interface {string}
    set status [enable|disable]
end

```

config system dedicated-mgmt

Parameter	Description	Type	Size	Default
default-gateway	Default gateway for dedicated management interface.	ipv4-address	Not Specified	0.0.0.0
dhcp-end-ip	DHCP end IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0
dhcp-netmask	DHCP netmask.	ipv4-netmask	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
dhcp-server	Enable/disable DHCP server on management interface.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DHCP server on management port.		
	<i>disable</i>	Disable DHCP server on management port.		
dhcp-start-ip	DHCP start IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0
interface	Dedicated management interface.	string	Maximum length: 15	
status	Enable/disable dedicated management.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config system device-upgrade

Independent upgrades for managed devices.

```

config system device-upgrade
  Description: Independent upgrades for managed devices.
  edit <serial>
    set device-type [fortigate|fortiswitch|...]
    set failure-reason [none|internal|...]
    set ha-reboot-controller {string}
    set initial-version {user}
    config known-ha-members
      Description: Known members of the HA cluster. If a member is missing at upgrade time,
the upgrade will be cancelled.
      edit <serial>
        next
      end
    set maximum-minutes {integer}
    set next-path-index {integer}
    set setup-time {user}
    set starter-admin {string}
    set status [disabled|initialized|...]
    set time {user}
    set timing [immediate|scheduled]
    set upgrade-path {user}
    set vdom {string}
  
```

```
next
end
```

config system device-upgrade

Parameter	Description	Type	Size	Default
device-type	Fortinet device type.	option	-	fortigate
	Option	Description		
	<i>fortigate</i>	This device is a FortiGate.		
	<i>fortiswitch</i>	This device is a FortiSwitch.		
	<i>fortiap</i>	This device is a FortiAP.		
	<i>fortiextender</i>	This device is a FortiExtender.		
failure-reason	Upgrade failure reason.	option	-	none
	Option	Description		
	<i>none</i>	No failure.		
	<i>internal</i>	An internal error occurred.		
	<i>timeout</i>	The upgrade timed out.		
	<i>device-type-unsupported</i>	The device type was not supported by the FortiGate.		
	<i>download-failed</i>	The image could not be downloaded.		
	<i>device-missing</i>	The device was disconnected from the FortiGate.		
	<i>version-unavailable</i>	An image matching the device and version could not be found.		
	<i>staging-failed</i>	The image could not be pushed to the device.		
	<i>reboot-failed</i>	The device could not be rebooted.		
	<i>device-not-reconnected</i>	The device did not reconnect after rebooting.		
	<i>node-not-ready</i>	A device in the Security Fabric tree was not ready.		
	<i>no-final-confirmation</i>	The coordinating FortiGate did not confirm the upgrade.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-confirmation-query</i></td><td>A downstream FortiGate did not initiate final confirmation.</td></tr><tr><td><i>config-error-log-nonempty</i></td><td>Configuration errors encountered during the upgrade.</td></tr><tr><td><i>csf-tree-not-supported</i></td><td>The Security Fabric is disabled on the root FortiGate</td></tr><tr><td><i>firmware-changed</i></td><td>Firmware changed after the upgrade was set up.</td></tr><tr><td><i>node-failed</i></td><td>A device in the Security Fabric tree failed.</td></tr></table>	Option	Description	<i>no-confirmation-query</i>	A downstream FortiGate did not initiate final confirmation.	<i>config-error-log-nonempty</i>	Configuration errors encountered during the upgrade.	<i>csf-tree-not-supported</i>	The Security Fabric is disabled on the root FortiGate	<i>firmware-changed</i>	Firmware changed after the upgrade was set up.	<i>node-failed</i>	A device in the Security Fabric tree failed.			
	Option	Description														
	<i>no-confirmation-query</i>	A downstream FortiGate did not initiate final confirmation.														
	<i>config-error-log-nonempty</i>	Configuration errors encountered during the upgrade.														
	<i>csf-tree-not-supported</i>	The Security Fabric is disabled on the root FortiGate														
	<i>firmware-changed</i>	Firmware changed after the upgrade was set up.														
<i>node-failed</i>	A device in the Security Fabric tree failed.															
ha-reboot-controller	Serial number of the FortiGate unit that will control the reboot process for the federated upgrade of the HA cluster.	string	Maximum length: 79													
initial-version	Firmware version when the upgrade was set up.	user	Not Specified													
maximum-minutes	Maximum number of minutes to allow for immediate upgrade preparation.	integer	Minimum value: 5 Maximum value: 10080	15												
next-path-index	The index of the next image to upgrade to.	integer	Minimum value: 0 Maximum value: 10	0												
serial	Serial number of the node to include.	string	Maximum length: 79													
setup-time	Upgrade preparation start time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified													
starter-admin	Admin that started the upgrade.	string	Maximum length: 64													
status	Current status of the upgrade.	option	-	disabled												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>No federated upgrade has been configured.</td></tr><tr><td><i>initialized</i></td><td>The upgrade has been configured.</td></tr></table>	Option	Description	<i>disabled</i>	No federated upgrade has been configured.	<i>initialized</i>	The upgrade has been configured.									
	Option	Description														
	<i>disabled</i>	No federated upgrade has been configured.														
<i>initialized</i>	The upgrade has been configured.															

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>downloading</i></td><td>The image is downloading in preparation for the upgrade.</td></tr><tr><td><i>device-disconnected</i></td><td>The image downloads are complete, but one or more devices have disconnected.</td></tr><tr><td><i>ready</i></td><td>The image download finished and the upgrade is pending.</td></tr><tr><td><i>coordinating</i></td><td>The upgrade is coordinating with other running upgrades.</td></tr><tr><td><i>staging</i></td><td>The upgrade is confirmed and images are being staged.</td></tr><tr><td><i>final-check</i></td><td>The upgrade is ready and final checks are in progress.</td></tr><tr><td><i>upgrade-devices</i></td><td>The upgrade is ready and devices are being rebooted.</td></tr><tr><td><i>cancelled</i></td><td>The upgrade was cancelled due to the tree not being ready.</td></tr><tr><td><i>confirmed</i></td><td>The upgrade was confirmed and reboots are running.</td></tr><tr><td><i>done</i></td><td>The upgrade completed successfully.</td></tr><tr><td><i>dry-run-done</i></td><td>The dry run finished.</td></tr><tr><td><i>failed</i></td><td>The upgrade failed due to a local issue.</td></tr></table>	Option	Description	<i>downloading</i>	The image is downloading in preparation for the upgrade.	<i>device-disconnected</i>	The image downloads are complete, but one or more devices have disconnected.	<i>ready</i>	The image download finished and the upgrade is pending.	<i>coordinating</i>	The upgrade is coordinating with other running upgrades.	<i>staging</i>	The upgrade is confirmed and images are being staged.	<i>final-check</i>	The upgrade is ready and final checks are in progress.	<i>upgrade-devices</i>	The upgrade is ready and devices are being rebooted.	<i>cancelled</i>	The upgrade was cancelled due to the tree not being ready.	<i>confirmed</i>	The upgrade was confirmed and reboots are running.	<i>done</i>	The upgrade completed successfully.	<i>dry-run-done</i>	The dry run finished.	<i>failed</i>	The upgrade failed due to a local issue.			
	Option	Description																												
	<i>downloading</i>	The image is downloading in preparation for the upgrade.																												
	<i>device-disconnected</i>	The image downloads are complete, but one or more devices have disconnected.																												
	<i>ready</i>	The image download finished and the upgrade is pending.																												
	<i>coordinating</i>	The upgrade is coordinating with other running upgrades.																												
	<i>staging</i>	The upgrade is confirmed and images are being staged.																												
	<i>final-check</i>	The upgrade is ready and final checks are in progress.																												
	<i>upgrade-devices</i>	The upgrade is ready and devices are being rebooted.																												
	<i>cancelled</i>	The upgrade was cancelled due to the tree not being ready.																												
	<i>confirmed</i>	The upgrade was confirmed and reboots are running.																												
	<i>done</i>	The upgrade completed successfully.																												
	<i>dry-run-done</i>	The dry run finished.																												
<i>failed</i>	The upgrade failed due to a local issue.																													
time	Scheduled upgrade execution time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified																											
timing	Run immediately or at a scheduled time.	option	-	immediate																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>immediate</i></td><td>Begin the upgrade immediately.</td></tr><tr><td><i>scheduled</i></td><td>Begin the upgrade at a configured time.</td></tr></table>	Option	Description	<i>immediate</i>	Begin the upgrade immediately.	<i>scheduled</i>	Begin the upgrade at a configured time.																							
	Option	Description																												
	<i>immediate</i>	Begin the upgrade immediately.																												
<i>scheduled</i>	Begin the upgrade at a configured time.																													
upgrade-path	Fortinet OS image versions to upgrade through in major-minor-patch format, such as 7-0-4.	user	Not Specified																											
vdom	Limit upgrade to this virtual domain (VDOM).	string	Maximum length: 31																											

config known-ha-members

Parameter	Description	Type	Size	Default
serial	Serial number of HA member	string	Maximum length: 79	

config system dhcp server

Configure DHCP servers.

```
config system dhcp server
  Description: Configure DHCP servers.
  edit <id>
    set auto-configuration [disable|enable]
    set auto-managed-status [disable|enable]
    set conflicted-ip-timeout {integer}
    set ddns-auth [disable|tsig]
    set ddns-key {password_aes256}
    set ddns-keyname {string}
    set ddns-server-ip {ipv4-address}
    set ddns-ttl {integer}
    set ddns-update [disable|enable]
    set ddns-update-override [disable|enable]
    set ddns-zone {string}
    set default-gateway {ipv4-address}
    set dhcp-settings-from-fortiipam [disable|enable]
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set dns-server3 {ipv4-address}
    set dns-server4 {ipv4-address}
    set dns-service [local|default|...]
    set domain {string}
  config exclude-range
    Description: Exclude one or more ranges of IP addresses from being assigned to
clients.
    edit <id>
      set end-ip {ipv4-address}
      set lease-time {integer}
      set start-ip {ipv4-address}
      set uci-match [disable|enable]
      set uci-string <uci-string1>, <uci-string2>, ...
      set vci-match [disable|enable]
      set vci-string <vci-string1>, <vci-string2>, ...
    next
  end
  set filename {string}
  set forticlient-on-net-status [disable|enable]
  set interface {string}
  set ip-mode [range|usrgrp]
  config ip-range
    Description: DHCP IP range configuration.
    edit <id>
      set end-ip {ipv4-address}
      set lease-time {integer}
      set start-ip {ipv4-address}
      set uci-match [disable|enable]
      set uci-string <uci-string1>, <uci-string2>, ...
```

```

        set vci-match [disable|enable]
        set vci-string <vci-string1>, <vci-string2>, ...
    next
end
set ipsec-lease-hold {integer}
set lease-time {integer}
set mac-acl-default-action [assign|block]
set netmask {ipv4-netmask}
set next-server {ipv4-address}
set ntp-server1 {ipv4-address}
set ntp-server2 {ipv4-address}
set ntp-server3 {ipv4-address}
set ntp-service [local|default|...]
config options
    Description: DHCP options.
    edit <id>
        set code {integer}
        set ip {user}
        set type [hex|string|...]
        set uci-match [disable|enable]
        set uci-string <uci-string1>, <uci-string2>, ...
        set value {string}
        set vci-match [disable|enable]
        set vci-string <vci-string1>, <vci-string2>, ...
    next
end
set relay-agent {ipv4-address}
config reserved-address
    Description: Options for the DHCP server to assign IP settings to specific MAC
addresses.
    edit <id>
        set action [assign|block|...]
        set circuit-id {string}
        set circuit-id-type [hex|string]
        set description {var-string}
        set ip {ipv4-address}
        set mac {mac-address}
        set remote-id {string}
        set remote-id-type [hex|string]
        set type [mac|option82]
    next
end
set server-type [regular|ipsec]
set shared-subnet [disable|enable]
set status [disable|enable]
set tftp-server <tftp-server1>, <tftp-server2>, ...
set timezone {string}
set timezone-option [disable|default|...]
set vci-match [disable|enable]
set vci-string <vci-string1>, <vci-string2>, ...
set wifi-ac-service [specify|local]
set wifi-ac1 {ipv4-address}

```

```

set wifi-ac2 {ipv4-address}
set wifi-ac3 {ipv4-address}
set wins-server1 {ipv4-address}
set wins-server2 {ipv4-address}
next
end

```

config system dhcp server

Parameter	Description	Type	Size	Default
auto-configuration	Enable/disable auto configuration.	option	-	enable
	Option		Description	
	<i>disable</i>		Disable auto configuration.	
	<i>enable</i>		Enable auto configuration.	
auto-managed-status	Enable/disable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.	option	-	enable
	Option		Description	
	<i>disable</i>		Disable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.	
	<i>enable</i>		Enable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.	
conflicted-ip-timeout	Time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be reused.	integer	Minimum value: 60 Maximum value: 8640000	1800
ddns-auth	DDNS authentication mode.	option	-	disable
	Option		Description	
	<i>disable</i>		Disable DDNS authentication.	
	<i>tsig</i>		TSIG based on RFC2845.	
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified	
ddns-keyname	DDNS update key name.	string	Maximum length: 64	
ddns-server-ip	DDNS server IP.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
ddns-ttl	TTL.	integer	Minimum value: 60 Maximum value: 86400	300
ddns-update	Enable/disable DDNS update for DHCP.	option	-	disable
	Option Description			
	disable Disable DDNS update for DHCP.			
	enable Enable DDNS update for DHCP.			
ddns-update-override	Enable/disable DDNS update override for DHCP.	option	-	disable
	Option Description			
	disable Disable DDNS update override for DHCP.			
	enable Enable DDNS update override for DHCP.			
ddns-zone	Zone of your domain name (ex. DDNS.com).	string	Maximum length: 64	
default-gateway	Default gateway IP address assigned by the DHCP server.	ipv4-address	Not Specified	0.0.0.0
dhcp-settings-from-fortiipam	Enable/disable populating of DHCP server settings from FortiIPAM.	option	-	disable
	Option Description			
	disable Disable populating of DHCP server settings from FortiIPAM.			
	enable Enable populating of DHCP server settings from FortiIPAM.			
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0
dns-server3	DNS server 3.	ipv4-address	Not Specified	0.0.0.0
dns-server4	DNS server 4.	ipv4-address	Not Specified	0.0.0.0
dns-service	Options for assigning DNS servers to DHCP clients.	option	-	specify

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.		
	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.		
	<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.		
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35	
filename	Name of the boot file on the TFTP server.	string	Maximum length: 127	
forticlient-on-net-status	Enable/disable FortiClient-On-Net service for this DHCP server.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable FortiClient On-Net Status.		
	<i>enable</i>	Enable FortiClient On-Net Status.		
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15	
ip-mode	Method used to assign client IP.	option	-	range
	Option	Description		
	<i>range</i>	Use range defined by start-ip/end-ip to assign client IP.		
	<i>usrgrp</i>	Use user-group defined method to assign client IP.		
ipsec-lease-hold	DHCP over IPsec leases expire this many seconds after tunnel down (0 to disable forced-expiry).	integer	Minimum value: 60 0 Maximum value: 8640000	
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
mac-acl-default-action	MAC access control default action (allow or block assigning IP settings).	option	-	assign

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>assign</i>	Allow the DHCP server to assign IP settings to clients on the MAC access control list.		
	<i>block</i>	Block the DHCP server from assigning IP settings to clients on the MAC access control list.		
netmask	Netmask assigned by the DHCP server.	ipv4-netmask	Not Specified	0.0.0.0
next-server	IP address of a server (for example, a TFTP sever) that DHCP clients can download a boot file from.	ipv4-address	Not Specified	0.0.0.0
ntp-server1	NTP server 1.	ipv4-address	Not Specified	0.0.0.0
ntp-server2	NTP server 2.	ipv4-address	Not Specified	0.0.0.0
ntp-server3	NTP server 3.	ipv4-address	Not Specified	0.0.0.0
ntp-service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients.	option	-	specify
	Option	Description		
	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.		
	<i>default</i>	Clients are assigned the FortiGate's configured NTP servers.		
	<i>specify</i>	Specify up to 3 NTP servers in the DHCP server configuration.		
relay-agent	Relay agent IP.	ipv4-address	Not Specified	0.0.0.0
server-type	DHCP server can be a normal DHCP server or an IPsec DHCP server.	option	-	regular
	Option	Description		
	<i>regular</i>	Regular DHCP service.		
	<i>ipsec</i>	DHCP over IPsec service.		
shared-subnet	Enable/disable shared subnet.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable shared subnet.</td></tr><tr><td><i>enable</i></td><td>Enable shared subnet.</td></tr></table>	Option	Description	<i>disable</i>	Disable shared subnet.	<i>enable</i>	Enable shared subnet.					
	Option	Description										
	<i>disable</i>	Disable shared subnet.										
<i>enable</i>	Enable shared subnet.											
status	Enable/disable this DHCP configuration.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not use this DHCP server configuration.</td></tr><tr><td><i>enable</i></td><td>Use this DHCP server configuration.</td></tr></table>	Option	Description	<i>disable</i>	Do not use this DHCP server configuration.	<i>enable</i>	Use this DHCP server configuration.					
	Option	Description										
	<i>disable</i>	Do not use this DHCP server configuration.										
<i>enable</i>	Use this DHCP server configuration.											
tftp-server <tftp-server>	One or more hostnames or IP addresses of the TFTP servers in quotes separated by spaces. TFTP server.	string	Maximum length: 63									
timezone	Select the time zone to be assigned to DHCP clients.	string	Maximum length: 63									
timezone-option	Options for the DHCP server to set the client's time zone.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not set the client's time zone.</td></tr><tr><td><i>default</i></td><td>Clients are assigned the FortiGate's configured time zone.</td></tr><tr><td><i>specify</i></td><td>Specify the time zone to be assigned to DHCP clients.</td></tr></table>	Option	Description	<i>disable</i>	Do not set the client's time zone.	<i>default</i>	Clients are assigned the FortiGate's configured time zone.	<i>specify</i>	Specify the time zone to be assigned to DHCP clients.			
	Option	Description										
	<i>disable</i>	Do not set the client's time zone.										
	<i>default</i>	Clients are assigned the FortiGate's configured time zone.										
<i>specify</i>	Specify the time zone to be assigned to DHCP clients.											
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable VCI matching.</td></tr><tr><td><i>enable</i></td><td>Enable VCI matching.</td></tr></table>	Option	Description	<i>disable</i>	Disable VCI matching.	<i>enable</i>	Enable VCI matching.					
	Option	Description										
	<i>disable</i>	Disable VCI matching.										
<i>enable</i>	Enable VCI matching.											
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255									
wifi-ac-service	Options for assigning WiFi access controllers to DHCP clients.	option	-	specify								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>specify</i>	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.		
	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.		
wifi-ac1	WiFi Access Controller 1 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0
wifi-ac2	WiFi Access Controller 2 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0
wifi-ac3	WiFi Access Controller 3 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0
wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0
wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0

config exclude-range

Parameter	Description	Type	Size	Default						
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0						
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0						
lease-time	Lease time in seconds, 0 means default lease time.	integer	Minimum value: 300 Maximum value: 8640000	0						
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0						
uci-match	Enable/disable user class identifier (UCI) matching. When enabled only DHCP requests with a matching UCI are served with this range.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable UCI matching.</td></tr><tr><td>enable</td><td>Enable UCI matching.</td></tr></table>				Option	Description	disable	Disable UCI matching.	enable	Enable UCI matching.
Option	Description									
disable	Disable UCI matching.									
enable	Enable UCI matching.									

Parameter	Description	Type	Size	Default
uci-string <uci-string>	One or more UCI strings in quotes separated by spaces. UCI strings.	string	Maximum length: 255	
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served with this range.	option	-	disable
	Option	Description		
	disable	Disable VCI matching.		
	enable	Enable VCI matching.		
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255	

config ip-range

Parameter	Description	Type	Size	Default						
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
lease-time	Lease time in seconds, 0 means default lease time.	integer	Minimum value: 300 Maximum value: 8640000	0						
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0						
uci-match	Enable/disable user class identifier (UCI) matching. When enabled only DHCP requests with a matching UCI are served with this range.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable UCI matching.</td></tr><tr><td>enable</td><td>Enable UCI matching.</td></tr></table>				Option	Description	disable	Disable UCI matching.	enable	Enable UCI matching.
Option	Description									
disable	Disable UCI matching.									
enable	Enable UCI matching.									
uci-string <uci-string>	One or more UCI strings in quotes separated by spaces. UCI strings.	string	Maximum length: 255							

Parameter	Description	Type	Size	Default
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served with this range.	option	-	disable
	Option Description			
	<i>disable</i>	Disable VCI matching.		
	<i>enable</i>	Enable VCI matching.		
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255	

config options

Parameter	Description	Type	Size	Default
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255	0
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	DHCP option IPs.	user	Not Specified	
type	DHCP option type.	option	-	hex
	Option Description			
	<i>hex</i>	DHCP option in hex.		
	<i>string</i>	DHCP option in string.		
	<i>ip</i>	DHCP option in IP.		
	<i>fqdn</i>	DHCP option in domain search option format.		
uci-match	Enable/disable user class identifier (UCI) matching. When enabled only DHCP requests with a matching UCI are served with this option.	option	-	disable
	Option Description			
	<i>disable</i>	Disable UCI matching.		
	<i>enable</i>	Enable UCI matching.		

Parameter	Description	Type	Size	Default						
uci-string <uci-string>	One or more UCI strings in quotes separated by spaces. UCI strings.	string	Maximum length: 255							
value	DHCP option value.	string	Maximum length: 312							
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served with this option.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable VCI matching.</td></tr><tr><td>enable</td><td>Enable VCI matching.</td></tr></table>				Option	Description	disable	Disable VCI matching.	enable	Enable VCI matching.
Option	Description									
disable	Disable VCI matching.									
enable	Enable VCI matching.									
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255							

config reserved-address

Parameter	Description	Type	Size	Default
action	Options for the DHCP server to configure the client with the reserved MAC address.	option	-	reserved
	Option	Description		
	<i>assign</i>	Configure the client with this MAC address like any other client.		
	<i>block</i>	Block the DHCP server from assigning IP settings to the client with this MAC address.		
	<i>reserved</i>	Assign the reserved IP address to the client with this MAC address.		
circuit-id	Option 82 circuit-ID of the client that will get the reserved IP address.	string	Maximum length: 312	
circuit-id-type	DHCP option type.	option	-	string
	Option	Description		
	<i>hex</i>	DHCP option in hex.		
	<i>string</i>	DHCP option in string.		
description	Description.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
ip	IP address to be reserved for the MAC address.	ipv4-address	Not Specified	0.0.0.0						
mac	MAC address of the client that will get the reserved IP address.	mac-address	Not Specified	00:00:00:00:00:00						
remote-id	Option 82 remote-ID of the client that will get the reserved IP address.	string	Maximum length: 312							
remote-id-type	DHCP option type.	option	-	string						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hex</td><td>DHCP option in hex.</td></tr><tr><td>string</td><td>DHCP option in string.</td></tr></table>				Option	Description	hex	DHCP option in hex.	string	DHCP option in string.
Option	Description									
hex	DHCP option in hex.									
string	DHCP option in string.									
type	DHCP reserved-address type.	option	-	mac						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mac</td><td>Match with MAC address.</td></tr><tr><td>option82</td><td>Match with DHCP option 82.</td></tr></table>				Option	Description	mac	Match with MAC address.	option82	Match with DHCP option 82.
Option	Description									
mac	Match with MAC address.									
option82	Match with DHCP option 82.									

config system dhcp6 server

Configure DHCPv6 servers.

```

config system dhcp6 server
  Description: Configure DHCPv6 servers.
  edit <id>
    set delegated-prefix-iaid {integer}
    set delegated-prefix-route [disable|enable]
    set dns-search-list [delegated|specify]
    set dns-server1 {ipv6-address}
    set dns-server2 {ipv6-address}
    set dns-server3 {ipv6-address}
    set dns-server4 {ipv6-address}
    set dns-service [delegated|default|...]
    set domain {string}
    set interface {string}
    set ip-mode [range|delegated]
    config ip-range

```

```

        Description: DHCP IP range configuration.
        edit <id>
            set end-ip {ipv6-address}
            set start-ip {ipv6-address}
            set vci-match [disable|enable]
            set vci-string <vci-string1>, <vci-string2>, ...
        next
    end
    set lease-time {integer}
    config options
        Description: DHCPv6 options.
        edit <id>
            set code {integer}
            set ip6 {user}
            set type [hex|string|...]
            set value {string}
            set vci-match [disable|enable]
            set vci-string <vci-string1>, <vci-string2>, ...
        next
    end
    set prefix-mode [dhcp6|ra]
    config prefix-range
        Description: DHCP prefix configuration.
        edit <id>
            set end-prefix {ipv6-address}
            set prefix-length {integer}
            set start-prefix {ipv6-address}
        next
    end
    set rapid-commit [disable|enable]
    set status [disable|enable]
    set subnet {ipv6-prefix}
    set upstream-interface {string}
next
end

```

config system dhcp6 server

Parameter	Description	Type	Size	Default
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0
delegated-prefix-route	Enable/disable automatically adding of routing for delegated prefix.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable automatically adding of routing for delegated prefix.</td></tr><tr><td><i>enable</i></td><td>Enable automatically adding of routing for delegated prefix.</td></tr></table>				Option	Description	<i>disable</i>	Disable automatically adding of routing for delegated prefix.	<i>enable</i>	Enable automatically adding of routing for delegated prefix.		
	Option	Description										
	<i>disable</i>	Disable automatically adding of routing for delegated prefix.										
<i>enable</i>	Enable automatically adding of routing for delegated prefix.											
dns-search-list	DNS search list options.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>delegated</i></td><td>Delegated the DNS search list.</td></tr><tr><td><i>specify</i></td><td>Specify the DNS search list.</td></tr></table>				Option	Description	<i>delegated</i>	Delegated the DNS search list.	<i>specify</i>	Specify the DNS search list.		
	Option	Description										
	<i>delegated</i>	Delegated the DNS search list.										
<i>specify</i>	Specify the DNS search list.											
dns-server1	DNS server 1.	ipv6-address	Not Specified	::								
dns-server2	DNS server 2.	ipv6-address	Not Specified	::								
dns-server3	DNS server 3.	ipv6-address	Not Specified	::								
dns-server4	DNS server 4.	ipv6-address	Not Specified	::								
dns-service	Options for assigning DNS servers to DHCPv6 clients.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>delegated</i></td><td>Delegated DNS settings.</td></tr><tr><td><i>default</i></td><td>Clients are assigned the FortiGate's configured DNS servers.</td></tr><tr><td><i>specify</i></td><td>Specify up to 3 DNS servers in the DHCPv6 server configuration.</td></tr></table>				Option	Description	<i>delegated</i>	Delegated DNS settings.	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.	<i>specify</i>	Specify up to 3 DNS servers in the DHCPv6 server configuration.
	Option	Description										
	<i>delegated</i>	Delegated DNS settings.										
	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.										
<i>specify</i>	Specify up to 3 DNS servers in the DHCPv6 server configuration.											
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35									
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295									
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15									
ip-mode	Method used to assign client IP.	option	-	range								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>range</i>	Use range defined by start IP/end IP to assign client IP.		
	<i>delegated</i>	Use delegated prefix method to assign client IP.		
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
prefix-mode	Assigning a prefix from a DHCPv6 client or RA.	option	-	dhcp6
	Option	Description		
	<i>dhcp6</i>	Use delegated prefix from a DHCPv6 client.		
	<i>ra</i>	Use prefix from RA.		
rapid-commit	Enable/disable allow/disallow rapid commit.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not allow rapid commit.		
	<i>enable</i>	Allow rapid commit.		
status	Enable/disable this DHCPv6 configuration.	option	-	enable
	Option	Description		
	<i>disable</i>	Enable this DHCPv6 server configuration.		
	<i>enable</i>	Disable this DHCPv6 server configuration.		
subnet	Subnet or subnet-id if the IP mode is delegated.	ipv6-prefix	Not Specified	::/0
upstream-interface	Interface name from where delegated information is provided.	string	Maximum length: 15	

config ip-range

Parameter	Description	Type	Size	Default
end-ip	End of IP range.	ipv6-address	Not Specified	::
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
start-ip	Start of IP range.	ipv6-address	Not Specified	::
vci-match	Enable/disable vendor class option matching. When enabled only DHCP requests with a matching VC are served with this range.	option	-	disable
	Option	Description		
	disable	Disable VCI matching.		
	enable	Enable VCI matching.		
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255	

config options

Parameter	Description	Type	Size	Default										
code	DHCPv6 option code.	integer	Minimum value: 0 0 Maximum value: 255	0										
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0										
ip6	DHCP option IP6s.	user	Not Specified											
type	DHCPv6 option type.	option	-	hex										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hex</td><td>DHCPv6 option in hex.</td></tr><tr><td>string</td><td>DHCPv6 option in string.</td></tr><tr><td>ip6</td><td>DHCPv6 option in IP6.</td></tr><tr><td>fqdn</td><td>DHCPv6 option in domain search option format.</td></tr></table>				Option	Description	hex	DHCPv6 option in hex.	string	DHCPv6 option in string.	ip6	DHCPv6 option in IP6.	fqdn	DHCPv6 option in domain search option format.
	Option	Description												
	hex	DHCPv6 option in hex.												
	string	DHCPv6 option in string.												
	ip6	DHCPv6 option in IP6.												
fqdn	DHCPv6 option in domain search option format.													
value	DHCPv6 option value (hexadecimal value must be even).	string	Maximum length: 312											
vci-match	Enable/disable vendor class option matching. When enabled only DHCP requests with a matching VCI are served with this option.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable VCI matching.		
	<i>enable</i>	Enable VCI matching.		
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255	

config prefix-range

Parameter	Description	Type	Size	Default
end-prefix	End of prefix range.	ipv6-address	Not Specified	::
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix-length	Prefix length.	integer	Minimum value: 1 Maximum value: 128	0
start-prefix	Start of prefix range.	ipv6-address	Not Specified	::

config system digital-io



This command is available for model(s): FortiGateRugged 70F 3G4G, FortiGateRugged 70F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure digital-io.

```
config system digital-io
  Description: Configure digital-io.
  set input1-detection-mode [default|voltage]
  set input2-detection-mode [default|voltage]
  set output-keep-last-state [enable|disable]
end
```

config system digital-io

Parameter	Description	Type	Size	Default
input1-detection-mode	Set input1 to default(open closed) or voltage (low high).	option	-	voltage
	Option	Description		
	default	Detecting open closed.		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>voltage</i></td><td>Detecting low high.</td></tr></table>	Option	Description	<i>voltage</i>	Detecting low high.					
	Option	Description								
	<i>voltage</i>	Detecting low high.								
input2-detection-mode	Set input2 to default(open closed) or voltage (low high).	option	-	voltage						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Detecting open closed.</td></tr><tr><td><i>voltage</i></td><td>Detecting low high.</td></tr></table>	Option	Description	<i>default</i>	Detecting open closed.	<i>voltage</i>	Detecting low high.			
	Option	Description								
	<i>default</i>	Detecting open closed.								
<i>voltage</i>	Detecting low high.									
output-keep-last-state	enable: keep the previous output state default opposite after reboot.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable config.</td></tr><tr><td><i>disable</i></td><td>Disable config.</td></tr></table>	Option	Description	<i>enable</i>	Enable config.	<i>disable</i>	Disable config.			
	Option	Description								
	<i>enable</i>	Enable config.								
<i>disable</i>	Disable config.									

config system dnp3-proxy



This command is available for model(s): FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure dnpproxy settings.

```
config system dnp3-proxy
  Description: Configure dnpproxy settings.
  set port {integer}
  set status [enable|disable]
  set term-baudrate [9600|19200|...]
  set term-databits {integer}
  set term-flowcontrol [none|xon_xoff|...]
  set term-parity [none|odd|...]
  set term-stopbits {integer}
end
```

config system dnp3-proxy

Parameter	Description	Type	Size	Default
port	DNP3 TCPServer Port.	integer	Minimum value: 1 Maximum value: 65535	20000
status	Enable/disable DNP daemon.	option	-	disable
	Option Description			
	<i>enable</i>	Enable DNP daemon.		
	<i>disable</i>	Disable DNP daemon.		
term-baudrate	Term Baudrate.	option	-	19200
	Option Description			
	<i>9600</i>	set DNP baudrate to 9600		
	<i>19200</i>	set DNP baudrate to 19200		
	<i>38400</i>	set DNP baudrate to 38400		
	<i>115200</i>	set DNP baudrate to 115200		
term-databits	Term Data Bits.	integer	Minimum value: 0 Maximum value: 65535	8
term-flowcontrol	Term Flow Control	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No flow control.		
	<i>xon_xoff</i>	Enable software flow control on both input and output.		
	<i>hardware</i>	Enable hardware flow control.		
term-parity	Term Parity	option	-	none
	Option	Description		
	<i>none</i>	No parity check.		
	<i>odd</i>	Odd parity check.		
	<i>even</i>	Even parity check.		
term-stopbits	Term Stop Bits.	integer	Minimum value: 0 Maximum value: 65535	1

config system dns

Configure DNS.

```

config system dns
  Description: Configure DNS.
  set alt-primary {ipv4-address}
  set alt-secondary {ipv4-address}
  set cache-notfound-responses [disable|enable]
  set dns-cache-limit {integer}
  set dns-cache-ttl {integer}
  set domain <domain1>, <domain2>, ...
  set fqdn-cache-ttl {integer}
  set fqdn-max-refresh {integer}
  set fqdn-min-refresh {integer}
  set hostname-limit {integer}
  set hostname-ttl {integer}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ip6-primary {ipv6-address}
  set ip6-secondary {ipv6-address}
  set log [disable|error|...]
  set primary {ipv4-address}
  set protocol {option1}, {option2}, ...
  set retry {integer}
  set root-servers {user}

```

```

set secondary {ipv4-address}
set server-hostname <hostname1>, <hostname2>, ...
set server-select-method [least-rtt|failover]
set source-ip {ipv4-address}
set source-ip-interface {string}
set ssl-certificate {string}
set timeout {integer}
set vrf-select {integer}
end

```

config system dns

Parameter	Description	Type	Size	Default						
alt-primary	Alternate primary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0						
alt-secondary	Alternate secondary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0						
cache-notfound-responses	Enable/disable response from the DNS server when a record is not in cache.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable cache NOTFOUND responses from DNS server.</td></tr><tr><td>enable</td><td>Enable cache NOTFOUND responses from DNS server.</td></tr></table>				Option	Description	disable	Disable cache NOTFOUND responses from DNS server.	enable	Enable cache NOTFOUND responses from DNS server.
Option	Description									
disable	Disable cache NOTFOUND responses from DNS server.									
enable	Enable cache NOTFOUND responses from DNS server.									
dns-cache-limit	Maximum number of records in the DNS cache.	integer	Minimum value: 0 Maximum value: 4294967295	5000						
dns-cache-ttl	Duration in seconds that the DNS cache retains information.	integer	Minimum value: 60 Maximum value: 86400	1800						
domain <domain>	Search suffix list for hostname lookup. DNS search domain list separated by space (maximum 8 domains).	string	Maximum length: 127							
fqdn-cache-ttl	FQDN cache time to live in seconds (0 - 86400, default = 0).	integer	Minimum value: 0 Maximum value: 86400	0						
fqdn-max-refresh	FQDN cache maximum refresh time in seconds (3600 - 86400, default = 3600).	integer	Minimum value: 3600 Maximum value: 86400	3600						

Parameter	Description	Type	Size	Default								
fqdn-min-refresh	FQDN cache minimum refresh time in seconds (10 - 3600, default = 60).	integer	Minimum value: 10 Maximum value: 3600	60								
hostname-limit	Limit of the number of hostname table entries (0 - 50000).	integer	Minimum value: 0 Maximum value: 50000	5000								
hostname-ttl	TTL of hostname table entries (60 - 86400).	integer	Minimum value: 60 Maximum value: 86400	86400								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
ip6-primary	Primary DNS server IPv6 address.	ipv6-address	Not Specified	::								
ip6-secondary	Secondary DNS server IPv6 address.	ipv6-address	Not Specified	::								
log	Local DNS log setting.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>error</td><td>Enable local DNS error log.</td></tr><tr><td>all</td><td>Enable local DNS log.</td></tr></table>				Option	Description	disable	Disable.	error	Enable local DNS error log.	all	Enable local DNS log.
Option	Description											
disable	Disable.											
error	Enable local DNS error log.											
all	Enable local DNS log.											
primary	Primary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0								
protocol	DNS transport protocols.	option	-	cleartext								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cleartext</td><td>DNS over UDP/53, DNS over TCP/53.</td></tr><tr><td>dot</td><td>DNS over TLS/853.</td></tr><tr><td>doh</td><td>DNS over HTTPS/443.</td></tr></table>				Option	Description	cleartext	DNS over UDP/53, DNS over TCP/53.	dot	DNS over TLS/853.	doh	DNS over HTTPS/443.
Option	Description											
cleartext	DNS over UDP/53, DNS over TCP/53.											
dot	DNS over TLS/853.											
doh	DNS over HTTPS/443.											

Parameter	Description	Type	Size	Default						
retry	Number of times to retry (0 - 5).	integer	Minimum value: 0 Maximum value: 5	2						
root-servers	Configure up to two preferred servers that serve the DNS root zone (default uses all 13 root servers).	user	Not Specified							
secondary	Secondary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0						
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127							
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>least-rtt</i></td><td>Select servers based on least round trip time.</td></tr><tr><td><i>failover</i></td><td>Select servers based on the order they are configured.</td></tr></table>				Option	Description	<i>least-rtt</i>	Select servers based on least round trip time.	<i>failover</i>	Select servers based on the order they are configured.
Option	Description									
<i>least-rtt</i>	Select servers based on least round trip time.									
<i>failover</i>	Select servers based on the order they are configured.									
source-ip	IP address used by the DNS server as its source IP.	ipv4-address	Not Specified	0.0.0.0						
source-ip-interface	IP address of the specified interface as the source IP address.	string	Maximum length: 15							
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory						
timeout	DNS query timeout interval in seconds (1 - 10).	integer	Minimum value: 1 Maximum value: 10	5						
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config system dns64

Configure DNS64.

```
config system dns64
  Description: Configure DNS64.
  set always-synthesize-aaaa-record [enable|disable]
  set dns64-prefix {ipv6-prefix}
```



```

    set status [enable|disable]
end

```

config system dns64

Parameter	Description	Type	Size	Default
always-synthesize-aaaa-record	Enable/disable AAAA record synthesis (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable AAAA record synthesis.		
	<i>disable</i>	Disable AAAA record synthesis.		
dns64-prefix	DNS64 prefix must be ::/96 (default = 64:ff9b::/96).	ipv6-prefix	Not Specified	64:ff9b::/96
status	Enable/disable DNS64 (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS64.		
	<i>disable</i>	Disable DNS64.		

config system dns-database

Configure DNS databases.

```

config system dns-database
    Description: Configure DNS databases.
    edit <name>
        set allow-transfer {user}
        set authoritative [enable|disable]
        set contact {string}
        config dns-entry
            Description: DNS entry.
            edit <id>
                set canonical-name {string}
                set hostname {string}
                set ip {ipv4-address-any}
                set ipv6 {ipv6-address}
                set preference {integer}
                set status [enable|disable]
                set ttl {integer}
                set type [A|NS|...]
            next
        next
    next

```

```

end
set domain {string}
set forwarder {user}
set forwarder6 {ipv6-address}
set interface {string}
set interface-select-method [auto|sdwan|...]
set ip-primary {ipv4-address-any}
set primary-name {string}
set rr-max {integer}
set source-ip {ipv4-address}
set source-ip-interface {string}
set source-ip6 {ipv6-address}
set status [enable|disable]
set ttl {integer}
set type [primary|secondary]
set view [shadow|public|...]
set vrf-select {integer}
next
end

```

config system dns-database

Parameter	Description	Type	Size	Default
allow-transfer	DNS zone transfer IP address list.	user	Not Specified	
authoritative	Enable/disable authoritative zone.	option	-	enable
	Option	Description		
	enable	Enable authoritative zone.		
	disable	Disable authoritative zone.		
contact	Email address of the administrator for this zone. You can specify only the username, such as admin or the full email address, such as admin@test.com When using only a username, the domain of the email will be this zone.	string	Maximum length: 255	host
domain	Domain name.	string	Maximum length: 255	
forwarder	DNS zone forwarder IP address list.	user	Not Specified	
forwarder6	Forwarder IPv6 address.	ipv6-address	Not Specified	::
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
	Option	Description										
	auto	Set outgoing interface automatically.										
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.										
specify	Set outgoing interface manually.											
ip-primary	IP address of primary DNS server. Entries in this primary DNS server and imported into the DNS zone.	ipv4-address-any	Not Specified	0.0.0.0								
name	Zone name.	string	Maximum length: 35									
primary-name	Domain name of the default DNS server for this zone.	string	Maximum length: 255	dns								
rr-max	Maximum number of resource records (10 - 65536, 0 means infinite).	integer	Minimum value: 10 Maximum value: 65536	16384								
source-ip	Source IP for forwarding to DNS server.	ipv4-address	Not Specified	0.0.0.0								
source-ip-interface	IP address of the specified interface as the source IP address.	string	Maximum length: 15									
source-ip6	IPv6 source IP address for forwarding to DNS server.	ipv6-address	Not Specified	::								
status	Enable/disable this DNS zone.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
ttl	Default time-to-live value for the entries of this DNS zone (0 - 2147483647 sec, default = 86400).	integer	Minimum value: 0 Maximum value: 2147483647	86400								
type	Zone type (primary to manage entries directly, secondary to import entries from other zones).	option	-	primary								

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>primary</i></td><td>Primary DNS zone, to manage entries directly.</td></tr><tr><td><i>secondary</i></td><td>Secondary DNS zone, to import entries from other DNS zones.</td></tr></table>	Option	Description	<i>primary</i>	Primary DNS zone, to manage entries directly.	<i>secondary</i>	Secondary DNS zone, to import entries from other DNS zones.							
	Option	Description												
	<i>primary</i>	Primary DNS zone, to manage entries directly.												
<i>secondary</i>	Secondary DNS zone, to import entries from other DNS zones.													
view	Zone view (public to serve public clients, shadow to serve internal clients).	option	-	shadow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shadow</i></td><td>Shadow DNS zone to serve internal clients.</td></tr><tr><td><i>public</i></td><td>Public DNS zone to serve public clients.</td></tr><tr><td><i>shadow-ztna</i></td><td>implicit DNS zone for ztna dox tunnel.</td></tr><tr><td><i>proxy</i></td><td>Shadow DNS zone for internal proxy.</td></tr></table>	Option	Description	<i>shadow</i>	Shadow DNS zone to serve internal clients.	<i>public</i>	Public DNS zone to serve public clients.	<i>shadow-ztna</i>	implicit DNS zone for ztna dox tunnel.	<i>proxy</i>	Shadow DNS zone for internal proxy.			
	Option	Description												
	<i>shadow</i>	Shadow DNS zone to serve internal clients.												
	<i>public</i>	Public DNS zone to serve public clients.												
	<i>shadow-ztna</i>	implicit DNS zone for ztna dox tunnel.												
<i>proxy</i>	Shadow DNS zone for internal proxy.													
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0										

config dns-entry

Parameter	Description	Type	Size	Default
canonical-name	Canonical name of the host.	string	Maximum length: 255	
hostname	Name of the host.	string	Maximum length: 255	
id	DNS entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the host.	ipv4-address-any	Not Specified	0.0.0.0
ipv6	IPv6 address of the host.	ipv6-address	Not Specified	::
preference	DNS entry preference (0 - 65535, highest preference = 0, default = 10).	integer	Minimum value: 0 Maximum value: 65535	10
status	Enable/disable resource record status.	option	-	enable

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable resource record status.</td></tr><tr><td><i>disable</i></td><td>Disable resource record status.</td></tr></table>	Option	Description	<i>enable</i>	Enable resource record status.	<i>disable</i>	Disable resource record status.													
	Option	Description																		
	<i>enable</i>	Enable resource record status.																		
<i>disable</i>	Disable resource record status.																			
ttl	Time-to-live for this entry (0 to 2147483647 sec, default = 0).	integer	Minimum value: 0 Maximum value: 2147483647	0																
type	Resource record type.	option	-	A																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>A</td><td>Host type.</td></tr><tr><td>NS</td><td>Name server type.</td></tr><tr><td>CNAME</td><td>Canonical name type.</td></tr><tr><td>MX</td><td>Mail exchange type.</td></tr><tr><td>AAAA</td><td>IPv6 host type.</td></tr><tr><td>PTR</td><td>Pointer type.</td></tr><tr><td>PTR_V6</td><td>IPv6 pointer type.</td></tr></table>	Option	Description	A	Host type.	NS	Name server type.	CNAME	Canonical name type.	MX	Mail exchange type.	AAAA	IPv6 host type.	PTR	Pointer type.	PTR_V6	IPv6 pointer type.			
	Option	Description																		
	A	Host type.																		
	NS	Name server type.																		
	CNAME	Canonical name type.																		
	MX	Mail exchange type.																		
	AAAA	IPv6 host type.																		
PTR	Pointer type.																			
PTR_V6	IPv6 pointer type.																			

config system dns-server

Configure DNS servers.

```

config system dns-server
    Description: Configure DNS servers.
    edit <name>
        set dnsfilter-profile {string}
        set doh [enable|disable]
        set doh3 [enable|disable]
        set doq [enable|disable]
        set mode [recursive|non-recursive|...]
    next
end

```

config system dns-server

Parameter	Description	Type	Size	Default
dnsfilter-profile	DNS filter profile.	string	Maximum length: 47	
doh	Enable/disable DNS over HTTPS/443 (default = disable).	option	-	disable
	Option	Description		
	enable	Enable DNS over HTTPS.		
	disable	Disable DNS over HTTPS.		
doh3	Enable/disable DNS over QUIC/HTTP3/443 (default = disable).	option	-	disable
	Option	Description		
	enable	Enable DNS over HTTP3/QUIC.		
	disable	Disable DNS over HTTP3/QUIC.		
doq	Enable/disable DNS over QUIC/853 (default = disable).	option	-	disable
	Option	Description		
	enable	Enable DNS over QUIC.		
	disable	Disable DNS over QUIC.		
mode	DNS server mode.	option	-	recursive
	Option	Description		
	recursive	Shadow DNS database and forward.		
	non-recursive	Public DNS database only.		
	forward-only	Forward only.		
	resolver	Recursive resolver mode.		
name	DNS server name.	string	Maximum length: 15	

config system dscp-based-priority

Configure DSCP based priority table.

```

config system dscp-based-priority
  Description: Configure DSCP based priority table.
  edit <id>
    set ds {integer}
    set priority [low|medium|...]
  next
end

```

config system dscp-based-priority

Parameter	Description	Type	Size	Default								
ds	DSCP(DiffServ) DS value (0 - 63).	integer	Minimum value: 0 0 Maximum value: 63	0								
id	Item ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0								
priority	DSCP based priority level.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>low</td><td>Low priority.</td></tr><tr><td>medium</td><td>Medium priority.</td></tr><tr><td>high</td><td>High priority.</td></tr></table>				Option	Description	low	Low priority.	medium	Medium priority.	high	High priority.
Option	Description											
low	Low priority.											
medium	Medium priority.											
high	High priority.											

config system elbc



This command is available for model(s): FortiGate 5001E1, FortiGate 5001E.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure enhanced load balance cluster.

```
config system elbc
    Description: Configure enhanced load balance cluster.
    set graceful-upgrade [enable|disable]
    set hb-device <name1>, <name2>, ...
    set inter-chassis-support [enable|disable]
    set mode [none|forticontroller|...]
end
```

config system elbc

Parameter	Description	Type	Size	Default
graceful-upgrade	enable/disable graceful upgrade	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default								
hb-device <name>	ELBC heartbeat device. set interface name	string	Maximum length: 79									
inter- chassis- support	Enable/disable content-cluster across multiple chassis.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable content-cluster across multiple chassis.</td></tr><tr><td><i>disable</i></td><td>Disable content-cluster across multiple chassis.</td></tr></table>				Option	Description	<i>enable</i>	Enable content-cluster across multiple chassis.	<i>disable</i>	Disable content-cluster across multiple chassis.		
Option	Description											
<i>enable</i>	Enable content-cluster across multiple chassis.											
<i>disable</i>	Disable content-cluster across multiple chassis.											
mode	ELBC mode.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>ELBC mode disabled.</td></tr><tr><td><i>forticontroller</i></td><td>FortiController.</td></tr><tr><td><i>dual- forticontroller</i></td><td>Dual-FortiController.</td></tr></table>				Option	Description	<i>none</i>	ELBC mode disabled.	<i>forticontroller</i>	FortiController.	<i>dual- forticontroller</i>	Dual-FortiController.
Option	Description											
<i>none</i>	ELBC mode disabled.											
<i>forticontroller</i>	FortiController.											
<i>dual- forticontroller</i>	Dual-FortiController.											

config system email-server

Configure the email server used by the FortiGate various things. For example, for sending email messages to users to support user authentication features.

```
config system email-server
    Description: Configure the email server used by the FortiGate various things. For example, for
    sending email messages to users to support user authentication features.
    set authenticate [enable|disable]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set password {password}
    set port {integer}
    set security [none|starttls|...]
    set server {string}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set ssl-min-proto-version [default|SSLv3|...]
    set type {option}
    set username {string}
    set validate-server [enable|disable]
    set vrf-select {integer}
end
```

config system email-server

Parameter	Description	Type	Size	Default								
authenticate	Enable/disable authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable authentication.</td></tr><tr><td>disable</td><td>Disable authentication.</td></tr></table>	Option	Description	enable	Enable authentication.	disable	Disable authentication.					
Option	Description											
enable	Enable authentication.											
disable	Disable authentication.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
password	SMTP server user password for authentication.	password	Not Specified									
port	SMTP server port.	integer	Minimum value: 1 Maximum value: 65535	25								
security	Connection security used by the email server.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>None.</td></tr><tr><td>starttls</td><td>STARTTLS.</td></tr><tr><td>smtps</td><td>SSL/TLS.</td></tr></table>	Option	Description	none	None.	starttls	STARTTLS.	smtps	SSL/TLS.			
Option	Description											
none	None.											
starttls	STARTTLS.											
smtps	SSL/TLS.											
server	SMTP server IP address or hostname.	string	Maximum length: 63									
source-ip	SMTP server IPv4 source IP.	ipv4-address	Not Specified	0.0.0.0								
source-ip6	SMTP server IPv6 source IP.	ipv6-address	Not Specified	::								

Parameter	Description	Type	Size	Default														
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
type	Use FortiGuard Message service or custom email server.	option	-	custom														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>custom</td><td>Use custom email server.</td></tr></table>	Option	Description	custom	Use custom email server.													
Option	Description																	
custom	Use custom email server.																	
username	SMTP server user name for authentication.	string	Maximum length: 255															
validate-server	Enable/disable validation of server certificate.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable validation of server certificate.</td></tr><tr><td>disable</td><td>Disable validation of server certificate.</td></tr></table>	Option	Description	enable	Enable validation of server certificate.	disable	Disable validation of server certificate.											
Option	Description																	
enable	Enable validation of server certificate.																	
disable	Disable validation of server certificate.																	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0														

config system evpn

Configure EVPN instance.

```
config system evpn
  Description: Configure EVPN instance.
  edit <id>
    set arp-suppression [enable|disable]
    set export-rt <route-target1>, <route-target2>, ...
```

```

        set import-rt <route-target1>, <route-target2>, ...
        set ip-local-learning [enable|disable]
        set rd {string}
    next
end

```

config system evpn

Parameter	Description	Type	Size	Default						
arp-suppression	Enable/disable ARP suppression.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ARP suppression.</td></tr><tr><td>disable</td><td>Disable ARP suppression.</td></tr></table>	Option	Description	enable	Enable ARP suppression.	disable	Disable ARP suppression.			
Option	Description									
enable	Enable ARP suppression.									
disable	Disable ARP suppression.									
export-rt <route-target>	List of export route targets. Route target: AA:NN A.B.C.D:NN.	string	Maximum length: 79							
id	ID.	integer	Minimum value: 1 Maximum value: 65535	0						
import-rt <route-target>	List of import route targets. Route target: AA:NN A.B.C.D:NN.	string	Maximum length: 79							
ip-local-learning	Enable/disable IP address local learning.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IP address local learning.</td></tr><tr><td>disable</td><td>Disable IP address local learning.</td></tr></table>	Option	Description	enable	Enable IP address local learning.	disable	Disable IP address local learning.			
Option	Description									
enable	Enable IP address local learning.									
disable	Disable IP address local learning.									
rd	Route Distinguisher: AA:NN A.B.C.D:NN.	string	Maximum length: 79							

config system external-resource

Configure external resource.

```

config system external-resource
    Description: Configure external resource.
    edit <name>
        set address-comment-field {string}
        set address-data-field {string}
        set address-name-field {string}
        set category {integer}
        set client-cert {string}
        set client-cert-auth [enable|disable]
        set comments {var-string}
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set namespace {string}
        set object-array-path {string}
        set password {password}
        set refresh-rate {integer}
        set resource {string}
        set server-identity-check [none|basic|...]
        set source-ip {ipv4-address}
        set status [enable|disable]
        set type [category|domain|...]
        set update-method [feed|push]
        set user-agent {var-string}
        set username {string}
        set uuid {uuid}
        set vrf-select {integer}
    next
end

```

config system external-resource

Parameter	Description	Type	Size	Default
address-comment-field	JSON Path to address description in generic address entry.	string	Maximum length: 511	\$.description
address-data-field	JSON Path to address data in generic address entry.	string	Maximum length: 511	\$.value
address-name-field	JSON Path to address name in generic address entry.	string	Maximum length: 511	\$.name
category	User resource category.	integer	Minimum value: 192 Maximum value: 221	0
client-cert	Client certificate name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
client-cert-auth	Enable/disable using client certificate for TLS authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable using client certificate for TLS authentication.		
	<i>disable</i>	Disable using client certificate for TLS authentication.		
comments	Comment.	var-string	Maximum length: 255	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
name	External resource name.	string	Maximum length: 35	
namespace	Generic external connector address namespace.	string	Maximum length: 15	
object-array-path	JSON Path to array of generic addresses in resource.	string	Maximum length: 511	\$.addresses
password	HTTP basic authentication password.	password	Not Specified	
refresh-rate	Time interval to refresh external resource (1 - 43200 min, default = 5 min).	integer	Minimum value: 1 Maximum value: 43200	5
resource	URL of external resource.	string	Maximum length: 511	
server-identity-check	Certificate verification option.	option	-	none

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No certificate verification.</td></tr><tr><td><i>basic</i></td><td>Check server certificate only.</td></tr><tr><td><i>full</i></td><td>Check server certificate and verify the domain matches in the server certificate.</td></tr></table>		Option	Description	<i>none</i>	No certificate verification.	<i>basic</i>	Check server certificate only.	<i>full</i>	Check server certificate and verify the domain matches in the server certificate.										
	Option	Description																		
	<i>none</i>	No certificate verification.																		
	<i>basic</i>	Check server certificate only.																		
<i>full</i>	Check server certificate and verify the domain matches in the server certificate.																			
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified	0.0.0.0																
status	Enable/disable user resource.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user resource.</td></tr><tr><td><i>disable</i></td><td>Disable user resource.</td></tr></table>		Option	Description	<i>enable</i>	Enable user resource.	<i>disable</i>	Disable user resource.												
	Option	Description																		
	<i>enable</i>	Enable user resource.																		
<i>disable</i>	Disable user resource.																			
type	User resource type.	option	-	category																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>category</i></td><td>FortiGuard category.</td></tr><tr><td><i>domain</i></td><td>Domain Name.</td></tr><tr><td><i>malware</i></td><td>Malware hash.</td></tr><tr><td><i>address</i></td><td>Firewall IP address.</td></tr><tr><td><i>mac-address</i></td><td>Firewall MAC address.</td></tr><tr><td><i>data</i></td><td>Data file.</td></tr><tr><td><i>generic-address</i></td><td>Generic addresses.</td></tr></table>		Option	Description	<i>category</i>	FortiGuard category.	<i>domain</i>	Domain Name.	<i>malware</i>	Malware hash.	<i>address</i>	Firewall IP address.	<i>mac-address</i>	Firewall MAC address.	<i>data</i>	Data file.	<i>generic-address</i>	Generic addresses.		
	Option	Description																		
	<i>category</i>	FortiGuard category.																		
	<i>domain</i>	Domain Name.																		
	<i>malware</i>	Malware hash.																		
	<i>address</i>	Firewall IP address.																		
	<i>mac-address</i>	Firewall MAC address.																		
	<i>data</i>	Data file.																		
<i>generic-address</i>	Generic addresses.																			
update-method	External resource update method.	option	-	feed																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>feed</i></td><td>FortiGate unit will pull update from the external resource.</td></tr><tr><td><i>push</i></td><td>External Resource update is pushed to the FortiGate unit through the FortiGate unit's RESTAPI/CLI.</td></tr></table>		Option	Description	<i>feed</i>	FortiGate unit will pull update from the external resource.	<i>push</i>	External Resource update is pushed to the FortiGate unit through the FortiGate unit's RESTAPI/CLI.												
	Option	Description																		
<i>feed</i>	FortiGate unit will pull update from the external resource.																			
<i>push</i>	External Resource update is pushed to the FortiGate unit through the FortiGate unit's RESTAPI/CLI.																			
user-agent	HTTP User-Agent header (default = 'curl/7.58.0').	var-string	Maximum length: 255																	
username	HTTP basic authentication user name.	string	Maximum length: 64																	

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config system fabric-vpn

Setup for self orchestrated fabric auto discovery VPN.

```

config system fabric-vpn
  Description: Setup for self orchestrated fabric auto discovery VPN.
  config advertised-subnets
    Description: Local advertised subnets.
    edit <id>
      set access [inbound|bidirectional]
      set bgp-network {integer}
      set firewall-address {string}
      set policies {integer}
      set prefix {ipv4-classnet}
    next
  end
  set bgp-as {user}
  set branch-name {string}
  set health-checks {string}
  set loopback-address-block {ipv4-classnet-host}
  set loopback-advertised-subnet {integer}
  set loopback-interface {string}
  config overlays
    Description: Local overlay interfaces table.
    edit <name>
      set bgp-neighbor {string}
      set bgp-neighbor-group {string}
      set bgp-neighbor-range {integer}
      set bgp-network {integer}
      set interface {string}
      set ipsec-network-id {integer}
      set ipsec-phase1 {string}
      set overlay-policy {integer}
      set overlay-tunnel-block {ipv4-classnet-host}
      set remote-gw {ipv4-address-any}
      set route-policy {integer}
      set sdwan-member {integer}
    next
  end

```



```

set policy-rule [health-check|manual|...]
set psksecret {password-3}
set sdwan-zone {string}
set status [enable|disable]
set sync-mode [enable|disable]
set vpn-role [hub|spoke]
end

```

config system fabric-vpn

Parameter	Description	Type	Size	Default								
bgp-as	BGP Router AS number, asplain/asdot/asdot+ format.	user	Not Specified									
branch-name	Branch name.	string	Maximum length: 35									
health-checks	Underlying health checks.	string	Maximum length: 35									
loopback-address-block	IPv4 address and subnet mask for hub's loopback address, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								
loopback-advertised-subnet	Loopback advertised subnet reference.	integer	Minimum value: 0 Maximum value: 4294967295	0								
loopback-interface	Loopback interface.	string	Maximum length: 15									
policy-rule	Policy creation rule.	option	-	health-check								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>health-check</td><td>Create health check policy automatically.</td></tr><tr><td>manual</td><td>All policies will be created manually.</td></tr><tr><td>auto</td><td>Automatically create allow policies.</td></tr></table>				Option	Description	health-check	Create health check policy automatically.	manual	All policies will be created manually.	auto	Automatically create allow policies.
Option	Description											
health-check	Create health check policy automatically.											
manual	All policies will be created manually.											
auto	Automatically create allow policies.											
psksecret	Pre-shared secret for ADVPN.	password-3	Not Specified									
sdwan-zone	Reference to created SD-WAN zone.	string	Maximum length: 35									
status	Enable/disable Fabric VPN.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Fabric VPN.		
	<i>disable</i>	Disable Fabric VPN.		
sync-mode	Setting synchronised by fabric or manual.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable fabric led configuration synchronisation.		
	<i>disable</i>	Disable fabric led configuration synchronisation.		
vpn-role	Fabric VPN role.	option	-	hub
	Option	Description		
	<i>hub</i>	VPN hub.		
	<i>spoke</i>	VPN spoke.		

config advertised-subnets

Parameter	Description	Type	Size	Default
access	Access policy direction.	option	-	inbound
	Option	Description		
	<i>inbound</i>	Allow inbound traffic to subnet.		
	<i>bidirectional</i>	Allow inbound and outbound traffic to subnet.		
bgp-network	Underlying BGP network.	integer	Minimum value: 0 0 Maximum value: 4294967295	
firewall-address	Underlying firewall address.	string	Maximum length: 79	
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967294	
policies	Underlying policies.	integer	Minimum value: 0 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config overlays

Parameter	Description	Type	Size	Default
bgp-neighbor	Underlying BGP neighbor entry.	string	Maximum length: 45	
bgp-neighbor-group	Underlying BGP neighbor group entry.	string	Maximum length: 45	
bgp-neighbor-range	Underlying BGP neighbor range entry.	integer	Minimum value: 0 0 Maximum value: 4294967295	
bgp-network	Underlying BGP network.	integer	Minimum value: 0 0 Maximum value: 4294967295	
interface	Underlying interface name.	string	Maximum length: 15	
ipsec-network-id	VPN gateway network ID.	integer	Minimum value: 0 0 Maximum value: 255	
ipsec-phase1	IPsec interface.	string	Maximum length: 35	
name	Overlay name.	string	Maximum length: 79	
overlay-policy	The overlay policy to allow ADVPN thru traffic.	integer	Minimum value: 0 0 Maximum value: 4294967295	
overlay-tunnel-block	IPv4 address and subnet mask for the overlay tunnel , syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
remote-gw	IP address of the hub gateway (Set by hub).	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
route-policy	Underlying router policy.	integer	Minimum value: 0 Maximum value: 4294967295	0
sdwan-member	Reference to SD-WAN member entry.	integer	Minimum value: 0 Maximum value: 4294967295	0

config system federated-upgrade

Coordinate federated upgrades within the Security Fabric.

```

config system federated-upgrade
    Description: Coordinate federated upgrades within the Security Fabric.
    set failure-device {string}
    set failure-reason [none|internal|...]
    set ha-reboot-controller {string}
    set ignore-signing-errors [enable|disable]
    set initial-version {user}
    config known-ha-members
        Description: Known members of the HA cluster. If a member is missing at upgrade time, the
        upgrade will be cancelled.
        edit <serial>
            next
        end
    set next-path-index {integer}
    config node-list
        Description: Nodes which will be included in the upgrade.
        edit <serial>
            set coordinating-fortigate {string}
            set device-type [fortigate|fortiswitch|...]
            set failure-reason [none|internal|...]
            set maximum-minutes {integer}
            set setup-time {user}
            set time {user}
            set timing [immediate|scheduled]
            set upgrade-path {user}
        next
    end
    set source [user|auto-firmware-upgrade]
    set starter-admin {string}
    set status [disabled|initialized|...]
    set upgrade-id {integer}
end

```

config system federated-upgrade

Parameter	Description	Type	Size	Default
failure-device	Serial number of the node to include.	string	Maximum length: 79	
failure-reason	Reason for upgrade failure.	option	-	none

Option	Description
<i>none</i>	No failure.
<i>internal</i>	An internal error occurred.
<i>timeout</i>	The upgrade timed out.
<i>device-type-unsupported</i>	The device type was not supported by the FortiGate.
<i>download-failed</i>	The image could not be downloaded.
<i>device-missing</i>	The device was disconnected from the FortiGate.
<i>version-unavailable</i>	An image matching the device and version could not be found.
<i>staging-failed</i>	The image could not be pushed to the device.
<i>reboot-failed</i>	The device could not be rebooted.
<i>device-not-reconnected</i>	The device did not reconnect after rebooting.
<i>node-not-ready</i>	A device in the Security Fabric tree was not ready.
<i>no-final-confirmation</i>	The coordinating FortiGate did not confirm the upgrade.
<i>no-confirmation-query</i>	A downstream FortiGate did not initiate final confirmation.
<i>config-error-log-nonempty</i>	Configuration errors encountered during the upgrade.
<i>csf-tree-not-supported</i>	The Security Fabric is disabled on the root FortiGate
<i>firmware-changed</i>	Firmware changed after the upgrade was set up.
<i>node-failed</i>	A device in the Security Fabric tree failed.

Parameter	Description	Type	Size	Default																		
ha-reboot-controller	Serial number of the FortiGate unit that will control the reboot process for the federated upgrade of the HA cluster.	string	Maximum length: 79																			
ignore-signing-errors	Allow/reject use of FortiGate firmware images that are unsigned.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow use of FortiGate images that are unsigned.</td></tr><tr><td>disable</td><td>Reject use of FortiGate images that are unsigned.</td></tr></table>	Option	Description	enable	Allow use of FortiGate images that are unsigned.	disable	Reject use of FortiGate images that are unsigned.															
Option	Description																					
enable	Allow use of FortiGate images that are unsigned.																					
disable	Reject use of FortiGate images that are unsigned.																					
initial-version	Firmware version when the upgrade was set up.	user	Not Specified																			
next-path-index	The index of the next image to upgrade to.	integer	Minimum value: 0 Maximum value: 10	0																		
source	Source that set up the federated upgrade config.	option	-	user																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>user</td><td>Upgrade configured based on user input.</td></tr><tr><td>auto-firmware-upgrade</td><td>Upgrade configured by the FortiGuard auto-firmware-upgrade feature.</td></tr></table>	Option	Description	user	Upgrade configured based on user input.	auto-firmware-upgrade	Upgrade configured by the FortiGuard auto-firmware-upgrade feature.															
Option	Description																					
user	Upgrade configured based on user input.																					
auto-firmware-upgrade	Upgrade configured by the FortiGuard auto-firmware-upgrade feature.																					
starter-admin	Admin that started the upgrade.	string	Maximum length: 64																			
status	Current status of the upgrade.	option	-	disabled																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disabled</td><td>No federated upgrade has been configured.</td></tr><tr><td>initialized</td><td>The upgrade has been configured.</td></tr><tr><td>downloading</td><td>The image is downloading in preparation for the upgrade.</td></tr><tr><td>device-disconnected</td><td>The image downloads are complete, but one or more devices have disconnected.</td></tr><tr><td>ready</td><td>The image download finished and the upgrade is pending.</td></tr><tr><td>coordinating</td><td>The upgrade is coordinating with other running upgrades.</td></tr><tr><td>staging</td><td>The upgrade is confirmed and images are being staged.</td></tr><tr><td>final-check</td><td>The upgrade is ready and final checks are in progress.</td></tr></table>	Option	Description	disabled	No federated upgrade has been configured.	initialized	The upgrade has been configured.	downloading	The image is downloading in preparation for the upgrade.	device-disconnected	The image downloads are complete, but one or more devices have disconnected.	ready	The image download finished and the upgrade is pending.	coordinating	The upgrade is coordinating with other running upgrades.	staging	The upgrade is confirmed and images are being staged.	final-check	The upgrade is ready and final checks are in progress.			
Option	Description																					
disabled	No federated upgrade has been configured.																					
initialized	The upgrade has been configured.																					
downloading	The image is downloading in preparation for the upgrade.																					
device-disconnected	The image downloads are complete, but one or more devices have disconnected.																					
ready	The image download finished and the upgrade is pending.																					
coordinating	The upgrade is coordinating with other running upgrades.																					
staging	The upgrade is confirmed and images are being staged.																					
final-check	The upgrade is ready and final checks are in progress.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>upgrade-devices</i>	The upgrade is ready and devices are being rebooted.		
	<i>cancelled</i>	The upgrade was cancelled due to the tree not being ready.		
	<i>confirmed</i>	The upgrade was confirmed and reboots are running.		
	<i>done</i>	The upgrade completed successfully.		
	<i>dry-run-done</i>	The dry run finished.		
	<i>failed</i>	The upgrade failed due to a local issue.		
upgrade-id	Unique identifier for this upgrade.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config known-ha-members

Parameter	Description	Type	Size	Default
serial	Serial number of HA member	string	Maximum length: 79	

config node-list

Parameter	Description	Type	Size	Default
coordinating-fortigate	Serial number of the FortiGate unit that controls this device.	string	Maximum length: 79	
device-type	Fortinet device type.	option	-	fortigate
	Option	Description		
	<i>fortigate</i>	This device is a FortiGate.		
	<i>fortiswitch</i>	This device is a FortiSwitch.		
	<i>fortiap</i>	This device is a FortiAP.		
	<i>fortiextender</i>	This device is a FortiExtender.		
failure-reason	Upgrade failure reason.	option	-	none
	Option	Description		
	<i>none</i>	No failure.		

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>internal</i></td><td>An internal error occurred.</td></tr><tr><td><i>timeout</i></td><td>The upgrade timed out.</td></tr><tr><td><i>device-type-unsupported</i></td><td>The device type was not supported by the FortiGate.</td></tr><tr><td><i>download-failed</i></td><td>The image could not be downloaded.</td></tr><tr><td><i>device-missing</i></td><td>The device was disconnected from the FortiGate.</td></tr><tr><td><i>version-unavailable</i></td><td>An image matching the device and version could not be found.</td></tr><tr><td><i>staging-failed</i></td><td>The image could not be pushed to the device.</td></tr><tr><td><i>reboot-failed</i></td><td>The device could not be rebooted.</td></tr><tr><td><i>device-not-reconnected</i></td><td>The device did not reconnect after rebooting.</td></tr><tr><td><i>node-not-ready</i></td><td>A device in the Security Fabric tree was not ready.</td></tr><tr><td><i>no-final-confirmation</i></td><td>The coordinating FortiGate did not confirm the upgrade.</td></tr><tr><td><i>no-confirmation-query</i></td><td>A downstream FortiGate did not initiate final confirmation.</td></tr><tr><td><i>config-error-log-nonempty</i></td><td>Configuration errors encountered during the upgrade.</td></tr><tr><td><i>csf-tree-not-supported</i></td><td>The Security Fabric is disabled on the root FortiGate</td></tr><tr><td><i>firmware-changed</i></td><td>Firmware changed after the upgrade was set up.</td></tr><tr><td><i>node-failed</i></td><td>A device in the Security Fabric tree failed.</td></tr></table>	Option	Description	<i>internal</i>	An internal error occurred.	<i>timeout</i>	The upgrade timed out.	<i>device-type-unsupported</i>	The device type was not supported by the FortiGate.	<i>download-failed</i>	The image could not be downloaded.	<i>device-missing</i>	The device was disconnected from the FortiGate.	<i>version-unavailable</i>	An image matching the device and version could not be found.	<i>staging-failed</i>	The image could not be pushed to the device.	<i>reboot-failed</i>	The device could not be rebooted.	<i>device-not-reconnected</i>	The device did not reconnect after rebooting.	<i>node-not-ready</i>	A device in the Security Fabric tree was not ready.	<i>no-final-confirmation</i>	The coordinating FortiGate did not confirm the upgrade.	<i>no-confirmation-query</i>	A downstream FortiGate did not initiate final confirmation.	<i>config-error-log-nonempty</i>	Configuration errors encountered during the upgrade.	<i>csf-tree-not-supported</i>	The Security Fabric is disabled on the root FortiGate	<i>firmware-changed</i>	Firmware changed after the upgrade was set up.	<i>node-failed</i>	A device in the Security Fabric tree failed.			
	Option	Description																																				
	<i>internal</i>	An internal error occurred.																																				
	<i>timeout</i>	The upgrade timed out.																																				
	<i>device-type-unsupported</i>	The device type was not supported by the FortiGate.																																				
	<i>download-failed</i>	The image could not be downloaded.																																				
	<i>device-missing</i>	The device was disconnected from the FortiGate.																																				
	<i>version-unavailable</i>	An image matching the device and version could not be found.																																				
	<i>staging-failed</i>	The image could not be pushed to the device.																																				
	<i>reboot-failed</i>	The device could not be rebooted.																																				
	<i>device-not-reconnected</i>	The device did not reconnect after rebooting.																																				
	<i>node-not-ready</i>	A device in the Security Fabric tree was not ready.																																				
	<i>no-final-confirmation</i>	The coordinating FortiGate did not confirm the upgrade.																																				
	<i>no-confirmation-query</i>	A downstream FortiGate did not initiate final confirmation.																																				
	<i>config-error-log-nonempty</i>	Configuration errors encountered during the upgrade.																																				
	<i>csf-tree-not-supported</i>	The Security Fabric is disabled on the root FortiGate																																				
	<i>firmware-changed</i>	Firmware changed after the upgrade was set up.																																				
<i>node-failed</i>	A device in the Security Fabric tree failed.																																					
maximum-minutes	Maximum number of minutes to allow for immediate upgrade preparation.	integer	Minimum value: 5 Maximum value: 10080	15																																		
serial	Serial number of the node to include.	string	Maximum length: 79																																			

Parameter	Description	Type	Size	Default
setup-time	Upgrade preparation start time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified	
time	Scheduled upgrade execution time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified	
timing	Run immediately or at a scheduled time.	option	-	immediate
	Option	Description		
	immediate	Begin the upgrade immediately.		
	scheduled	Begin the upgrade at a configured time.		
upgrade-path	Fortinet OS image versions to upgrade through in major-minor-patch format, such as 7-0-4.	user	Not Specified	

config system fips-cc

Configure FIPS-CC mode.

```
config system fips-cc
  Description: Configure FIPS-CC mode.
  set key-generation-self-test [enable|disable]
  set self-test-period {integer}
  set status [enable|disable]
end
```

config system fips-cc

Parameter	Description	Type	Size	Default
key-generation-self-test	Enable/disable self tests after key generation.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable self tests after key generation.		
	<i>disable</i>	Disable self tests after key generation.		
self-test-period	Self test period.	integer	Minimum value: 1 Maximum value: 1440	1440
status	Enable/disable ciphers for FIPS mode of operation.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable FIPS-CC mode.		
	<i>disable</i>	Disable FIPS-CC mode.		

config system fortiguard

Configure FortiGuard services.

```
config system fortiguard
    Description: Configure FortiGuard services.
    set FDS-license-expiring-days {integer}
    set antispam-cache [enable|disable]
    set antispam-cache-mper mille {integer}
    set antispam-cache-ttl {integer}
    set antispam-expiration {integer}
    set antispam-force-off [enable|disable]
    set antispam-license {integer}
    set antispam-timeout {integer}
    set anycast-sdns-server-ip {ipv4-address}
    set anycast-sdns-server-port {integer}
    set auto-firmware-upgrade [enable|disable]
    set auto-firmware-upgrade-day {option1}, {option2}, ...
    set auto-firmware-upgrade-delay {integer}
    set auto-firmware-upgrade-end-hour {integer}
    set auto-firmware-upgrade-start-hour {integer}
    set auto-join-forticloud [enable|disable]
    set ddns-server-ip {ipv4-address}
    set ddns-server-ip6 {ipv6-address}
    set ddns-server-port {integer}
    set fortiguard-anycast [enable|disable]
    set fortiguard-anycast-source [fortinet|aws|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set load-balance-servers {integer}
    set outbreak-prevention-cache [enable|disable]
    set outbreak-prevention-cache-mper mille {integer}
    set outbreak-prevention-cache-ttl {integer}
    set outbreak-prevention-expiration {integer}
    set outbreak-prevention-force-off [enable|disable]
    set outbreak-prevention-license {integer}
    set outbreak-prevention-timeout {integer}
    set persistent-connection [enable|disable]
    set port [8888|53|...]
    set protocol [udp|http|...]
    set proxy-password {password}
    set proxy-server-ip {string}
```

```

set proxy-server-port {integer}
set proxy-username {string}
set sandbox-inline-scan [enable|disable]
set sandbox-region {string}
set sdns-options {option1}, {option2}, ...
set sdns-server-ip {user}
set sdns-server-port {integer}
set service-account-id {string}
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set subscribe-update-notification [enable|disable]
set update-build-proxy [enable|disable]
set update-dldb [enable|disable]
set update-extdb [enable|disable]
set update-ffdb [enable|disable]
set update-server-location [automatic|usa|...]
set update-uwdb [enable|disable]
set vdom {string}
set vrf-select {integer}
set webfilter-cache [enable|disable]
set webfilter-cache-ttl {integer}
set webfilter-expiration {integer}
set webfilter-force-off [enable|disable]
set webfilter-license {integer}
set webfilter-timeout {integer}
end

```

config system fortiguard

Parameter	Description	Type	Size	Default						
FDS-license-expiring-days	Threshold for number of days before FortiGuard license expiration to generate license expiring event log (1 - 100 days, default = 15).	integer	Minimum value: 1 Maximum value: 100	15						
antispam-cache	Enable/disable FortiGuard antispam request caching. Uses a small amount of memory but improves performance.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiGuard antispam request caching.</td></tr><tr><td>disable</td><td>Disable FortiGuard antispam request caching.</td></tr></table>				Option	Description	enable	Enable FortiGuard antispam request caching.	disable	Disable FortiGuard antispam request caching.
Option	Description									
enable	Enable FortiGuard antispam request caching.									
disable	Disable FortiGuard antispam request caching.									
antispam-cache-mpermille	Maximum permille of FortiGate memory the antispam cache is allowed to use (1 - 150).	integer	Minimum value: 1 Maximum value: 150	1						

Parameter	Description	Type	Size	Default						
antispam-cache-ttl	Time-to-live for antispam cache entries in seconds (300 - 86400). Lower times reduce the cache size. Higher times may improve performance since the cache will have more entries.	integer	Minimum value: 300 Maximum value: 86400	1800						
antispam-expiration	Expiration date of the FortiGuard antispam contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0						
antispam-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Turn off the FortiGuard antispam service.</td></tr><tr><td>disable</td><td>Allow the FortiGuard antispam service.</td></tr></table>				Option	Description	enable	Turn off the FortiGuard antispam service.	disable	Allow the FortiGuard antispam service.
Option	Description									
enable	Turn off the FortiGuard antispam service.									
disable	Allow the FortiGuard antispam service.									
antispam-license	Interval of time between license checks for the FortiGuard antispam contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295						
antispam-timeout	Antispam query time out (1 - 30 sec, default = 7).	integer	Minimum value: 1 Maximum value: 30	7						
anycast-sdns-server-ip	IP address of the FortiGuard anycast DNS rating server.	ipv4-address	Not Specified	0.0.0.0						
anycast-sdns-server-port	Port to connect to on the FortiGuard anycast DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	853						
auto-firmware-upgrade	Enable/disable automatic patch-level firmware upgrade from FortiGuard. The FortiGate unit searches for new patches only in the same major and minor version.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable automatic patch-level firmware upgrade to latest version from FortiGuard.</td></tr><tr><td>disable</td><td>Disable automatic patch-level firmware upgrade to latest version from FortiGuard.</td></tr></table>				Option	Description	enable	Enable automatic patch-level firmware upgrade to latest version from FortiGuard.	disable	Disable automatic patch-level firmware upgrade to latest version from FortiGuard.
Option	Description									
enable	Enable automatic patch-level firmware upgrade to latest version from FortiGuard.									
disable	Disable automatic patch-level firmware upgrade to latest version from FortiGuard.									

Parameter	Description	Type	Size	Default																
auto-firmware-upgrade-day	Allowed day(s) of the week to install an automatic patch-level firmware upgrade from FortiGuard (default is none). Disallow any day of the week to use auto-firmware-upgrade-delay instead, which waits for designated days before installing an automatic patch-level firmware upgrade.	option	-																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday.</td></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr></table>	Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.			
	Option	Description																		
	<i>sunday</i>	Sunday.																		
	<i>monday</i>	Monday.																		
	<i>tuesday</i>	Tuesday.																		
	<i>wednesday</i>	Wednesday.																		
	<i>thursday</i>	Thursday.																		
	<i>friday</i>	Friday.																		
<i>saturday</i>	Saturday.																			
auto-firmware-upgrade-delay	Delay of day(s) before installing an automatic patch-level firmware upgrade from FortiGuard (default = 3). Set it 0 to use auto-firmware-upgrade-day instead, which selects allowed day(s) of the week for installing an automatic patch-level firmware upgrade.	integer	Minimum value: 3 0 Maximum value: 14																	
auto-firmware-upgrade-end-hour	End time in the designated time window for automatic patch-level firmware upgrade from FortiGuard in 24 hour time (0 ~ 23, default = 4). When the end time is smaller than the start time, the end time is interpreted as the next day. The actual upgrade time is selected randomly within the time window.	integer	Minimum value: 4 0 Maximum value: 23																	
auto-firmware-upgrade-start-hour	Start time in the designated time window for automatic patch-level firmware upgrade from FortiGuard in 24 hour time (0 ~ 23, default = 2). The actual upgrade time is selected randomly within the time window.	integer	Minimum value: 1 0 Maximum value: 23																	
auto-join-forticloud *	Automatically connect to and login to FortiCloud.	option	-	enable																

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatic connection and login to FortiCloud.		
	<i>disable</i>	Disable automatic connection and login to FortiCloud.		
ddns-server-ip	IP address of the FortiDDNS server.	ipv4-address	Not Specified	0.0.0.0
ddns-server-ip6	IPv6 address of the FortiDDNS server.	ipv6-address	Not Specified	::
ddns-server-port	Port used to communicate with FortiDDNS servers.	integer	Minimum value: 1 Maximum value: 65535	443
fortiguard-anycast	Enable/disable use of FortiGuard's Anycast network.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of FortiGuard's Anycast network.		
	<i>disable</i>	Disable use of FortiGuard's Anycast network.		
fortiguard-anycast-source	Configure which of Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. Default is Fortinet.	option	-	fortinet
	Option	Description		
	<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.		
	<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.		
	<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
load-balance-servers	Number of servers to alternate between as first FortiGuard option.	integer	Minimum value: 1 1 Maximum value: 266	
outbreak-prevention-cache	Enable/disable FortiGuard Virus Outbreak Prevention cache.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiGuard antivirus caching.		
	<i>disable</i>	Disable FortiGuard antivirus caching.		
outbreak-prevention-cache-mpermille	Maximum permille of memory FortiGuard Virus Outbreak Prevention cache can use (1 - 150 permille, default = 1).	integer	Minimum value: 1 1 Maximum value: 150	
outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries (300 - 86400 sec, default = 300).	integer	Minimum value: 300 300 Maximum value: 86400	
outbreak-prevention-expiration	Expiration date of FortiGuard Virus Outbreak Prevention contract. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295	
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-	disable
	Option	Description		
	<i>enable</i>	Turn off FortiGuard antivirus service.		
	<i>disable</i>	Allow the FortiGuard antivirus service.		
outbreak-prevention-license	Interval of time between license checks for FortiGuard Virus Outbreak Prevention contract. Read-only.	integer	Minimum value: 4294967295 0 Maximum value: 4294967295	
outbreak-prevention-timeout	FortiGuard Virus Outbreak Prevention time out (1 - 30 sec, default = 7).	integer	Minimum value: 7 1 Maximum value: 30	

Parameter	Description	Type	Size	Default										
persistent-connection	Enable/disable use of persistent connection to receive update notification from FortiGuard.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable persistent connection to receive update notification from FortiGuard.</td></tr><tr><td><i>disable</i></td><td>Disable persistent connection to receive update notification from FortiGuard.</td></tr></table>	Option	Description	<i>enable</i>	Enable persistent connection to receive update notification from FortiGuard.	<i>disable</i>	Disable persistent connection to receive update notification from FortiGuard.							
Option	Description													
<i>enable</i>	Enable persistent connection to receive update notification from FortiGuard.													
<i>disable</i>	Disable persistent connection to receive update notification from FortiGuard.													
port	Port used to communicate with the FortiGuard servers.	option	-	443										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>8888</i></td><td>port 8888 for server communication.</td></tr><tr><td><i>53</i></td><td>port 53 for server communication.</td></tr><tr><td><i>80</i></td><td>port 80 for server communication.</td></tr><tr><td><i>443</i></td><td>port 443 for server communication.</td></tr></table>	Option	Description	<i>8888</i>	port 8888 for server communication.	<i>53</i>	port 53 for server communication.	<i>80</i>	port 80 for server communication.	<i>443</i>	port 443 for server communication.			
Option	Description													
<i>8888</i>	port 8888 for server communication.													
<i>53</i>	port 53 for server communication.													
<i>80</i>	port 80 for server communication.													
<i>443</i>	port 443 for server communication.													
protocol	Protocol used to communicate with the FortiGuard servers.	option	-	https										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>UDP for server communication (for use by FortiGuard or FortiManager).</td></tr><tr><td><i>http</i></td><td>HTTP for server communication (for use only by FortiManager).</td></tr><tr><td><i>https</i></td><td>HTTPS for server communication (for use by FortiGuard or FortiManager).</td></tr></table>	Option	Description	<i>udp</i>	UDP for server communication (for use by FortiGuard or FortiManager).	<i>http</i>	HTTP for server communication (for use only by FortiManager).	<i>https</i>	HTTPS for server communication (for use by FortiGuard or FortiManager).					
Option	Description													
<i>udp</i>	UDP for server communication (for use by FortiGuard or FortiManager).													
<i>http</i>	HTTP for server communication (for use only by FortiManager).													
<i>https</i>	HTTPS for server communication (for use by FortiGuard or FortiManager).													
proxy-password	Proxy user password.	password	Not Specified											
proxy-server-ip	Hostname or IPv4 address of the proxy server.	string	Maximum length: 63											
proxy-server-port	Port used to communicate with the proxy server.	integer	Minimum value: 0 0 Maximum value: 65535											
proxy-username	Proxy user name.	string	Maximum length: 64											
sandbox-inline-scan *	Enable/disable FortiCloud Sandbox inline-scan.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable FortiCloud Sandbox inline scan.		
	<i>disable</i>	Disable FortiCloud Sandbox inline scan.		
sandbox-region	FortiCloud Sandbox region.	string	Maximum length: 63	
sdns-options	Customization options for the FortiGuard DNS service.	option	-	
	Option Description			
	<i>include-question-section</i>	Include DNS question section in the FortiGuard DNS setup message.		
sdns-server-ip	IP address of the FortiGuard DNS rating server.	user	Not Specified	
sdns-server-port	Port to connect to on the FortiGuard DNS rating server.	integer	Minimum value: 53 1 Maximum value: 65535	
service-account-id	Service account ID.	string	Maximum length: 50	
source-ip	Source IPv4 address used to communicate with FortiGuard.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used to communicate with FortiGuard.	ipv6-address	Not Specified	::
subscribe-update-notification	Enable/disable subscription to receive update notification from FortiGuard.	option	-	disable
	Option Description			
	<i>enable</i>	Enable subscription to receive update notification from FortiGuard.		
	<i>disable</i>	Disable subscription to receive update notification from FortiGuard.		
update-build-proxy	Enable/disable proxy dictionary rebuild.	option	-	enable
	Option Description			
	<i>enable</i>	Enable proxy dictionary rebuild.		
	<i>disable</i>	Disable proxy dictionary rebuild.		

Parameter	Description	Type	Size	Default								
update-dldb	Enable/disable DLP signature update.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP signature update.</td></tr><tr><td><i>disable</i></td><td>Disable DLP signature update.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP signature update.	<i>disable</i>	Disable DLP signature update.					
Option	Description											
<i>enable</i>	Enable DLP signature update.											
<i>disable</i>	Disable DLP signature update.											
update-extdb	Enable/disable external resource update.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable external resource update.</td></tr><tr><td><i>disable</i></td><td>Disable external resource update.</td></tr></table>	Option	Description	<i>enable</i>	Enable external resource update.	<i>disable</i>	Disable external resource update.					
Option	Description											
<i>enable</i>	Enable external resource update.											
<i>disable</i>	Disable external resource update.											
update-ffdb	Enable/disable Internet Service Database update.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Internet Service Database update.</td></tr><tr><td><i>disable</i></td><td>Disable Internet Service Database update.</td></tr></table>	Option	Description	<i>enable</i>	Enable Internet Service Database update.	<i>disable</i>	Disable Internet Service Database update.					
Option	Description											
<i>enable</i>	Enable Internet Service Database update.											
<i>disable</i>	Disable Internet Service Database update.											
update-server-location	Location from which to receive FortiGuard updates.	option	-	automatic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>automatic</i></td><td>FortiGuard servers chosen based on closest proximity to FortiGate unit.</td></tr><tr><td><i>usa</i></td><td>FortiGuard servers in United States.</td></tr><tr><td><i>eu</i></td><td>FortiGuard servers in the European Union.</td></tr></table>	Option	Description	<i>automatic</i>	FortiGuard servers chosen based on closest proximity to FortiGate unit.	<i>usa</i>	FortiGuard servers in United States.	<i>eu</i>	FortiGuard servers in the European Union.			
Option	Description											
<i>automatic</i>	FortiGuard servers chosen based on closest proximity to FortiGate unit.											
<i>usa</i>	FortiGuard servers in United States.											
<i>eu</i>	FortiGuard servers in the European Union.											
update-uwdb	Enable/disable allowlist update.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowlist update.</td></tr><tr><td><i>disable</i></td><td>Disable allowlist update.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowlist update.	<i>disable</i>	Disable allowlist update.					
Option	Description											
<i>enable</i>	Enable allowlist update.											
<i>disable</i>	Disable allowlist update.											
vdom	FortiGuard Service virtual domain name.	string	Maximum length: 31									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 0 Maximum value: 511									

Parameter	Description	Type	Size	Default
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable
	Option	Description		
	enable	Enable FortiGuard web filter caching.		
	disable	Disable FortiGuard web filter caching.		
webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds (300 - 86400).	integer	Minimum value: 300 Maximum value: 86400	3600
webfilter-expiration	Expiration date of the FortiGuard web filter contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable
	Option	Description		
	enable	Turn off the FortiGuard web filtering service.		
	disable	Allow the FortiGuard web filtering service to operate.		
webfilter-license	Interval of time between license checks for the FortiGuard web filter contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
webfilter-timeout	Web filter query time out (1 - 30 sec, default = 15).	integer	Minimum value: 1 Maximum value: 30	15

* This parameter may not exist in some models.

config system fortindr



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure FortiNDR.

```
config system fortindr
  Description: Configure FortiNDR.
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set source-ip {string}
  set status [disable|enable]
  set vrf-select {integer}
end
```

config system fortindr

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
source-ip	Source IP address for communications to FortiNDR.	string	Maximum length: 63									
status	Enable/disable FortiNDR.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FortiNDR.</td></tr><tr><td><i>enable</i></td><td>Enable FortiNDR.</td></tr></table>				Option	Description	<i>disable</i>	Disable FortiNDR.	<i>enable</i>	Enable FortiNDR.		
	Option	Description										
	<i>disable</i>	Disable FortiNDR.										
<i>enable</i>	Enable FortiNDR.											
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0								

config system fortisandbox

Configure FortiSandbox.

```

config system fortisandbox
  Description: Configure FortiSandbox.
  set ca {string}
  set certificate-verification [enable|disable]
  set cn {string}
  set email {string}
  set enc-algorithm [default|high|...]
  set forticloud [enable|disable]
  set inline-scan [enable|disable]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set server {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
  set vrf-select {integer}
end

```

config system fortisandbox

Parameter	Description	Type	Size	Default								
ca	The CA that signs remote FortiSandbox certificate, empty for no check.	string	Maximum length: 79									
certificate-verification	Enable/disable identity verification of FortiSandbox by use of certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable identity verification of FortiSandbox by use of certificate.</td></tr><tr><td>disable</td><td>Disable identity verification of FortiSandbox by use of certificate.</td></tr></table>				Option	Description	enable	Enable identity verification of FortiSandbox by use of certificate.	disable	Disable identity verification of FortiSandbox by use of certificate.		
Option	Description											
enable	Enable identity verification of FortiSandbox by use of certificate.											
disable	Disable identity verification of FortiSandbox by use of certificate.											
cn	The CN of remote server certificate, case sensitive, empty for no check.	string	Maximum length: 127									
email	Notifier email address.	string	Maximum length: 63									
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td>high</td><td>SSL communication with high encryption algorithms.</td></tr><tr><td>low</td><td>SSL communication with low encryption algorithms.</td></tr></table>				Option	Description	default	SSL communication with high and medium encryption algorithms.	high	SSL communication with high encryption algorithms.	low	SSL communication with low encryption algorithms.
Option	Description											
default	SSL communication with high and medium encryption algorithms.											
high	SSL communication with high encryption algorithms.											
low	SSL communication with low encryption algorithms.											
forticloud	Enable/disable FortiSandbox Cloud.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiSandbox Cloud.</td></tr><tr><td>disable</td><td>Disable FortiSandbox Cloud.</td></tr></table>				Option	Description	enable	Enable FortiSandbox Cloud.	disable	Disable FortiSandbox Cloud.		
Option	Description											
enable	Enable FortiSandbox Cloud.											
disable	Disable FortiSandbox Cloud.											
inline-scan *	Enable/disable FortiSandbox inline scan.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiSandbox inline scan.</td></tr><tr><td>disable</td><td>Disable FortiSandbox inline scan.</td></tr></table>				Option	Description	enable	Enable FortiSandbox inline scan.	disable	Disable FortiSandbox inline scan.		
Option	Description											
enable	Enable FortiSandbox inline scan.											
disable	Disable FortiSandbox inline scan.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
server	Server IP address or FQDN of the remote FortiSandbox.	string	Maximum length: 63	
source-ip	Source IP address for communications to FortiSandbox.	string	Maximum length: 63	
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
	<i>TLSv1-3</i>	TLSv1.3.		
status	Enable/disable FortiSandbox.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiSandbox.		
	<i>disable</i>	Disable FortiSandbox.		
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

* This parameter may not exist in some models.

config system fsso-polling

Configure Fortinet Single Sign On (FSSO) server.

```
config system fsso-polling
    Description: Configure Fortinet Single Sign On (FSSO) server.
```

```

set auth-password {password}
set authentication [enable|disable]
set listening-port {integer}
set status [enable|disable]
end

```

config system fssso-polling

Parameter	Description	Type	Size	Default						
auth-password	Password to connect to FSSO Agent.	password	Not Specified							
authentication	Enable/disable FSSO Agent Authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FSSO Agent Authentication.</td></tr><tr><td>disable</td><td>Disable FSSO Agent Authentication.</td></tr></table>				Option	Description	enable	Enable FSSO Agent Authentication.	disable	Disable FSSO Agent Authentication.
	Option	Description								
	enable	Enable FSSO Agent Authentication.								
disable	Disable FSSO Agent Authentication.									
listening-port	Listening port to accept clients (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	8000						
status	Enable/disable FSSO Polling Mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FSSO Polling Mode.</td></tr><tr><td>disable</td><td>Disable FSSO Polling Mode.</td></tr></table>				Option	Description	enable	Enable FSSO Polling Mode.	disable	Disable FSSO Polling Mode.
	Option	Description								
	enable	Enable FSSO Polling Mode.								
disable	Disable FSSO Polling Mode.									

config system ftm-push

Configure FortiToken Mobile push services.

```

config system ftm-push
  Description: Configure FortiToken Mobile push services.
  set proxy [enable|disable]
  set server {string}
  set server-cert {string}
  set server-ip {ipv4-address}
  set server-port {integer}
  set status [enable|disable]
end

```


config system ftm-push

Parameter	Description	Type	Size	Default
proxy	Enable/disable communication to the proxy server in FortiGuard configuration.	option	-	enable
	Option	Description		
	enable	Enable communication to the proxy server in FortiGuard configuration.		
	disable	Disable communication to the proxy server in FortiGuard configuration.		
server	IPv4 address or domain name of FortiToken Mobile push services server.	string	Maximum length: 127	
server-cert	Name of the server certificate to be used for SSL.	string	Maximum length: 35	Fortinet_GUI_Server
server-ip	IPv4 address of FortiToken Mobile push services server (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
server-port	Port to communicate with FortiToken Mobile push services server (1 - 65535, default = 4433).	integer	Minimum value: 1 Maximum value: 65535	4433
status	Enable/disable the use of FortiToken Mobile push services.	option	-	disable
	Option	Description		
	enable	Enable FortiToken Mobile push services.		
	disable	Disable FortiToken Mobile push services.		

config system geneve

Configure GENEVE devices.

```
config system geneve
  Description: Configure GENEVE devices.
  edit <name>
    set dstport {integer}
    set interface {string}
    set ip-version [ipv4-unicast|ipv6-unicast]
    set remote-ip {ipv4-address}
    set remote-ip6 {ipv6-address}
    set type [ethernet|ppp]
    set vni {integer}
```

```
next
end
```

config system geneve

Parameter	Description	Type	Size	Default						
dstport	GENEVE destination port (1 - 65535, default = 6081).	integer	Minimum value: 1 Maximum value: 65535	6081						
interface	Outgoing interface for GENEVE encapsulated traffic.	string	Maximum length: 15							
ip-version	IP version to use for the GENEVE interface and so for communication over the GENEVE. IPv4 or IPv6 unicast.	option	-	ipv4-unicast						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4-unicast</td><td>Use IPv4 unicast addressing over the GENEVE.</td></tr><tr><td>ipv6-unicast</td><td>Use IPv6 unicast addressing over the GENEVE.</td></tr></table>				Option	Description	ipv4-unicast	Use IPv4 unicast addressing over the GENEVE.	ipv6-unicast	Use IPv6 unicast addressing over the GENEVE.
Option	Description									
ipv4-unicast	Use IPv4 unicast addressing over the GENEVE.									
ipv6-unicast	Use IPv6 unicast addressing over the GENEVE.									
name	GENEVE device or interface name. Must be an unique interface name.	string	Maximum length: 15							
remote-ip	IPv4 address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv4-address	Not Specified	0.0.0.0						
remote-ip6	IPv6 IP address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv6-address	Not Specified	::						
type	GENEVE type.	option	-	ethernet						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ethernet</td><td>Internal packet includes Ethernet header.</td></tr><tr><td>ppp</td><td>Internal packet does not include Ethernet header.</td></tr></table>				Option	Description	ethernet	Internal packet includes Ethernet header.	ppp	Internal packet does not include Ethernet header.
Option	Description									
ethernet	Internal packet includes Ethernet header.									
ppp	Internal packet does not include Ethernet header.									
vni	GENEVE network ID.	integer	Minimum value: 0 Maximum value: 16777215	0						

config system geoip-override

Configure geographical location mapping for IP address(es) to override mappings from FortiGuard.

```

config system geoip-override
    Description: Configure geographical location mapping for IP address(es) to override mappings
    from FortiGuard.
    edit <name>
        set country-id {string}
        set description {string}
        config ip-range
            Description: Table of IP ranges assigned to country.
            edit <id>
                set end-ip {ipv4-address}
                set start-ip {ipv4-address}
            next
        end
        config ip6-range
            Description: Table of IPv6 ranges assigned to country.
            edit <id>
                set end-ip {ipv6-address}
                set start-ip {ipv6-address}
            next
        end
    next
end

```

config system geoip-override

Parameter	Description	Type	Size	Default
country-id	Two character Country ID code.	string	Maximum length: 2	
description	Description.	string	Maximum length: 127	
name	Location name.	string	Maximum length: 63	

config ip-range

Parameter	Description	Type	Size	Default
end-ip	Ending IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
id	ID of individual entry in the IP range table.	integer	Minimum value: 0 Maximum value: 65535	0
start-ip	Starting IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0

config ip6-range

Parameter	Description	Type	Size	Default
end-ip	Ending IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
id	ID of individual entry in the IPv6 range table.	integer	Minimum value: 0 Maximum value: 65535	0
start-ip	Starting IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::

config system global

Configure global attributes.

```
config system global
  Description: Configure global attributes.
  set admin-ble-button [enable|disable]
  set admin-concurrent [enable|disable]
  set admin-console-timeout {integer}
  set admin-forticloud-sso-default-profile {string}
  set admin-forticloud-sso-login [enable|disable]
  set admin-host {string}
  set admin-hsts-max-age {integer}
  set admin-https-pki-required [enable|disable]
  set admin-https-redirect [enable|disable]
  set admin-https-ssl-banned-ciphers {option1}, {option2}, ...
  set admin-https-ssl-ciphersuites {option1}, {option2}, ...
  set admin-https-ssl-versions {option1}, {option2}, ...
  set admin-lockout-duration {integer}
  set admin-lockout-threshold {integer}
  set admin-login-max {integer}
  set admin-port {integer}
  set admin-reset-button [enable|disable]
  set admin-restrict-local [all|non-console-only|...]
  set admin-scp [enable|disable]
  set admin-server-cert {string}
  set admin-sport {integer}
  set admin-ssh-grace-time {integer}
  set admin-ssh-password [enable|disable]
  set admin-ssh-port {integer}
  set admin-ssh-v1 [enable|disable]
  set admin-telnet [enable|disable]
  set admin-telnet-port {integer}
  set admintimeout {integer}
```

```
set airplane-mode [enable|disable]
set alias {string}
set allow-traffic-redirect [enable|disable]
set anti-replay [disable|loose|...]
set application-bandwidth-tracking [disable|enable]
set arp-max-entry {integer}
set auth-cert {string}
set auth-http-port {integer}
set auth-https-port {integer}
set auth-ike-saml-port {integer}
set auth-keepalive [enable|disable]
set auth-session-auto-backup [enable|disable]
set auth-session-auto-backup-interval [1min|5min|...]
set auth-session-limit [block-new|logout-inactive]
set auto-auth-extension-device [enable|disable]
set autorun-log-fsck [enable|disable]
set av-affinity {string}
set av-failopen [pass|off|...]
set av-failopen-session [enable|disable]
set batch-cmdb [enable|disable]
set bfd-affinity {string}
set block-session-timer {integer}
set br-fdb-max-entry {integer}
set cert-chain-max {integer}
set cfg-revert-timeout {integer}
set cfg-save [automatic|manual|...]
set check-protocol-header [loose|strict]
set check-reset-range [strict|disable]
set cli-audit-log [enable|disable]
set cloud-communication [enable|disable]
set clt-cert-req [enable|disable]
set cmdbsvr-affinity {string}
set cpu-use-threshold {integer}
set csr-ca-attribute [enable|disable]
set daily-restart [enable|disable]
set default-service-source-port {user}
set delay-tcp-npu-session [enable|disable]
set device-idle-timeout {integer}
set dh-params [1024|1536|...]
set dhcp-lease-backup-interval {integer}
set dnsproxy-worker-count {integer}
set early-tcp-npu-session [enable|disable]
set edit-vdom-prompt [enable|disable]
set extender-controller-reserved-network {ipv4-classnet-host}
set failtime {integer}
set faz-disk-buffer-size {integer}
set fds-statistics [enable|disable]
set fds-statistics-period {integer}
set fgd-alert-subscription {option1}, {option2}, ...
set forticontroller-proxy [enable|disable]
set forticontroller-proxy-port {integer}
set forticonverter-config-upload [once|disable]
```

```

set forticonverter-integration [enable|disable]
set fortiextender [disable|enable]
set fortiextender-data-port {integer}
set fortiextender-discovery-lockdown [disable|enable]
set fortiextender-provision-on-authorization [enable|disable]
set fortiextender-vlan-mode [enable|disable]
set fortigslb-integration [disable|enable]
set fortiservice-port {integer}
set fortitoken-cloud [enable|disable]
set fortitoken-cloud-push-status [enable|disable]
set fortitoken-cloud-sync-interval {integer}
set gtpu-dynamic-source-port [enable|disable]
set gui-allow-incompatible-fabric-fgt [enable|disable]
set gui-app-detection-sdwan [enable|disable]
set gui-auto-upgrade-setup-warning [enable|disable]
set gui-cdn-domain-override {string}
set gui-cdn-usage [enable|disable]
set gui-certificates [enable|disable]
set gui-custom-language [enable|disable]
set gui-date-format [yyyy/MM/dd|dd/MM/yyyy|...]
set gui-date-time-source [system|browser]
set gui-device-latitude {string}
set gui-device-longitude {string}
set gui-display-hostname [enable|disable]
set gui-firmware-upgrade-warning [enable|disable]
set gui-forticare-registration-setup-warning [enable|disable]
set gui-fortigate-cloud-sandbox [enable|disable]
set gui-ipv6 [enable|disable]
set gui-local-out [enable|disable]
set gui-replacement-message-groups [enable|disable]
set gui-rest-api-cache [enable|disable]
set gui-theme [jade|neutrino|...]
set gui-wireless-opensecurity [enable|disable]
set gui-workflow-management [enable|disable]
set ha-affinity {string}
set honor-df [enable|disable]
set hostname {string}
set httpd-max-worker-count {integer}
set hyper-scale-vdom-num {integer}
set igmp-state-limit {integer}
set interface-subnet-usage [disable|enable]
set internet-service-database [mini|standard|...]
set internet-service-download-list <id1>, <id2>, ...
set interval {integer}
set ip-conflict-detection [enable|disable]
set ip-fragment-mem-thresholds {integer}
set ip-fragment-timeout {integer}
set ip-src-port-range {user}
set ips-affinity {string}
set ipsec-asic-offload [enable|disable]
set ipsec-ha-seqjump-rate {integer}
set ipsec-hmac-offload [enable|disable]

```

```

set ipsec-qat-offload [enable|disable]
set ipv6-accept-dad {integer}
set ipv6-allow-anycast-probe [enable|disable]
set ipv6-allow-local-in-silent-drop [enable|disable]
set ipv6-allow-multicast-probe [enable|disable]
set ipv6-allow-traffic-redirect [enable|disable]
set ipv6-fragment-timeout {integer}
set irq-time-accounting [auto|force]
set language [english|french|...]
set ldapconntimeout {integer}
set legacy-poe-device-support [enable|disable]
set lldp-reception [enable|disable]
set lldp-transmission [enable|disable]
set log-single-cpu-high [enable|disable]
set log-ssl-connection [enable|disable]
set log-uuid-address [enable|disable]
set login-timestamp [enable|disable]
set long-vdom-name [enable|disable]
set management-ip {string}
set management-port {integer}
set management-port-use-admin-sport [enable|disable]
set management-vdom {string}
set max-route-cache-size {integer}
set memory-use-threshold-extreme {integer}
set memory-use-threshold-green {integer}
set memory-use-threshold-red {integer}
set miglog-affinity {string}
set miglogd-children {integer}
set multi-factor-authentication [optional|mandatory]
set ndp-max-entry {integer}
set npu-neighbor-update [enable|disable]
set per-user-bal [enable|disable]
set pmtu-discovery [enable|disable]
set policy-auth-concurrent {integer}
set post-login-banner [disable|enable]
set pre-login-banner [enable|disable]
set private-data-encryption [disable|enable]
set proxy-auth-lifetime [enable|disable]
set proxy-auth-lifetime-timeout {integer}
set proxy-auth-timeout {integer}
set proxy-cert-use-mgmt-vdom [enable|disable]
set proxy-hardware-acceleration [disable|enable]
set proxy-keep-alive-mode [session|traffic|...]
set proxy-re-authentication-time {integer}
set proxy-resource-mode [enable|disable]
set proxy-worker-count {integer}
set purdue-level [1|1.5|...]
set quic-ack-threshold {integer}
set quic-congestion-control-algo [cubic|bbr|...]
set quic-max-datagram-size {integer}
set quic-pmtud [enable|disable]
set quic-tls-handshake-timeout {integer}

```

```

set quic-udp-payload-size-shaping-per-cid [enable|disable]
set radius-port {integer}
set reboot-upon-config-restore [enable|disable]
set refresh {integer}
set remoteauthtimeout {integer}
set reset-sessionless-tcp [enable|disable]
set rest-api-key-url-query [enable|disable]
set restart-time {user}
set revision-backup-on-logout [enable|disable]
set revision-image-auto-backup [enable|disable]
set scanunit-count {integer}
set scim-http-port {integer}
set scim-https-port {integer}
set scim-server-cert {string}
set send-pmtu-icmp [enable|disable]
set sflowd-max-children-num {integer}
set show-backplane-intf [enable|disable]
set single-vdom-npuvlink [enable|disable]
set snat-route-change [enable|disable]
set special-file-23-support [disable|enable]
set speedtest-server [enable|disable]
set speedtestd-ctrl-port {integer}
set speedtestd-server-port {integer}
set split-port {string}
config split-port-mode
    Description: Configure split port mode of ports.
    edit <interface>
        set split-mode [disable|4x10G|...]
    next
end
set ssd-trim-date {integer}
set ssd-trim-freq [never|hourly|...]
set ssd-trim-hour {integer}
set ssd-trim-min {integer}
set ssd-trim-weekday [sunday|monday|...]
set ssl-min-proto-version [SSLv3|TLSv1|...]
set ssl-static-key-ciphers [enable|disable]
set sslvpn-affinity {string}
set sslvpn-max-worker-count {integer}
set sslvpn-web-mode [enable|disable]
set strict-dirty-session-check [enable|disable]
set strong-crypto [enable|disable]
set switch-controller [disable|enable]
set switch-controller-reserved-network {ipv4-classnet-host}
set sys-perf-log-interval {integer}
set syslog-affinity {string}
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-option [enable|disable]
set tcp-rst-timer {integer}
set tcp-timewait-timer {integer}
set telemetry-controller [enable|disable]

```



```

set telemetry-data-port {integer}
set tftp [enable|disable]
set timezone {string}
set tls-session-cache [enable|disable]
set traffic-priority [tos|dscp]
set traffic-priority-level [low|medium|...]
set two-factor-email-expiry {integer}
set two-factor-fac-expiry {integer}
set two-factor-ftk-expiry {integer}
set two-factor-ftm-expiry {integer}
set two-factor-sms-expiry {integer}
set udp-idle-timer {integer}
set upgrade-report [enable|disable]
set url-filter-affinity {string}
set url-filter-count {integer}
set user-device-store-max-device-mem {integer}
set user-device-store-max-devices {integer}
set user-device-store-max-unified-mem {integer}
set user-device-store-max-users {integer}
set user-history-password-threshold {integer}
set vdom-mode [no-vdom|multi-vdom]
set vip-arp-range [unlimited|restricted]
set virtual-switch-vlan [enable|disable]
set wad-affinity {string}
set wad-csvc-cs-count {integer}
set wad-csvc-db-count {integer}
set wad-memory-change-granularity {integer}
set wad-p2s-max-body-size {integer}
set wad-restart-end-time {user}
set wad-restart-mode [none|time|...]
set wad-restart-start-time {user}
set wad-source-affinity [disable|enable]
set wad-worker-count {integer}
set wifi-ca-certificate {string}
set wifi-certificate {string}
set wimax-4g-usb [enable|disable]
set wireless-controller [enable|disable]
set wireless-controller-port {integer}
set wireless-mode [ac|client|...]

```

end

config system global

Parameter	Description	Type	Size	Default
admin-ble-button *	press the BLE button can enable BLE function	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Press the BLE button can enable BLE function		
	<i>disable</i>	Press the BLE button cannot enable BLE function		
admin-concurrent	Enable/disable concurrent administrator logins. Use policy-auth-concurrent for firewall authenticated users.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable admin concurrent login.		
	<i>disable</i>	Disable admin concurrent login.		
admin-console-timeout	Console login timeout that overrides the admin timeout value (15 - 300 seconds, default = 0, which disables the timeout).	integer	Minimum value: 0 15 Maximum value: 300	
admin-forticloud-sso-default-profile	Override access profile.	string	Maximum length: 35	
admin-forticloud-sso-login	Enable/disable FortiCloud admin login via SSO.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiCloud admin login via SSO.		
	<i>disable</i>	Disable FortiCloud admin login via SSO.		
admin-host	Administrative host for HTTP and HTTPS. When set, will be used in lieu of the client's Host header for any redirection.	string	Maximum length: 255	
admin-hsts-max-age	HTTPS Strict-Transport-Security header max-age in seconds. A value of 0 will reset any HSTS records in the browser.When admin-https-redirect is disabled the header max-age will be 0.	integer	Minimum value: 0 Maximum value: 2147483647	63072000

Parameter	Description	Type	Size	Default																								
admin-https-pki-required	Enable/disable admin login method. Enable to force administrators to provide a valid certificate to log in if PKI is enabled. Disable to allow administrators to log in with a certificate or password.	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.</td></tr><tr><td>disable</td><td>Admin users can login by providing a valid certificate or password.</td></tr></table>	Option	Description	enable	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.	disable	Admin users can login by providing a valid certificate or password.																					
Option	Description																											
enable	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.																											
disable	Admin users can login by providing a valid certificate or password.																											
admin-https-redirect	Enable/disable redirection of HTTP administration access to HTTPS.	option	-	enable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable redirecting HTTP administration access to HTTPS.</td></tr><tr><td>disable</td><td>Disable redirecting HTTP administration access to HTTPS.</td></tr></table>	Option	Description	enable	Enable redirecting HTTP administration access to HTTPS.	disable	Disable redirecting HTTP administration access to HTTPS.																					
Option	Description																											
enable	Enable redirecting HTTP administration access to HTTPS.																											
disable	Disable redirecting HTTP administration access to HTTPS.																											
admin-https-ssl-banned-ciphers	Select one or more cipher technologies that cannot be used in GUI HTTPS negotiations. Only applies to TLS 1.2 and below.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>RSA</td><td>Ban the use of cipher suites using RSA key.</td></tr><tr><td>DHE</td><td>Ban the use of cipher suites using authenticated ephemeral DH key agreement.</td></tr><tr><td>ECDHE</td><td>Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.</td></tr><tr><td>DSS</td><td>Ban the use of cipher suites using DSS authentication.</td></tr><tr><td>ECDSA</td><td>Ban the use of cipher suites using ECDSA authentication.</td></tr><tr><td>AES</td><td>Ban the use of cipher suites using either 128 or 256 bit AES.</td></tr><tr><td>AESGCM</td><td>Ban the use of cipher suites using AES in Galois Counter Mode (GCM).</td></tr><tr><td>CAMELLIA</td><td>Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.</td></tr><tr><td>3DES</td><td>Ban the use of cipher suites using triple DES.</td></tr><tr><td>SHA1</td><td>Ban the use of cipher suites using HMAC-SHA1.</td></tr><tr><td>SHA256</td><td>Ban the use of cipher suites using HMAC-SHA256.</td></tr></table>	Option	Description	RSA	Ban the use of cipher suites using RSA key.	DHE	Ban the use of cipher suites using authenticated ephemeral DH key agreement.	ECDHE	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.	DSS	Ban the use of cipher suites using DSS authentication.	ECDSA	Ban the use of cipher suites using ECDSA authentication.	AES	Ban the use of cipher suites using either 128 or 256 bit AES.	AESGCM	Ban the use of cipher suites using AES in Galois Counter Mode (GCM).	CAMELLIA	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.	3DES	Ban the use of cipher suites using triple DES.	SHA1	Ban the use of cipher suites using HMAC-SHA1.	SHA256	Ban the use of cipher suites using HMAC-SHA256.			
Option	Description																											
RSA	Ban the use of cipher suites using RSA key.																											
DHE	Ban the use of cipher suites using authenticated ephemeral DH key agreement.																											
ECDHE	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.																											
DSS	Ban the use of cipher suites using DSS authentication.																											
ECDSA	Ban the use of cipher suites using ECDSA authentication.																											
AES	Ban the use of cipher suites using either 128 or 256 bit AES.																											
AESGCM	Ban the use of cipher suites using AES in Galois Counter Mode (GCM).																											
CAMELLIA	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.																											
3DES	Ban the use of cipher suites using triple DES.																											
SHA1	Ban the use of cipher suites using HMAC-SHA1.																											
SHA256	Ban the use of cipher suites using HMAC-SHA256.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	SHA384	Ban the use of cipher suites using HMAC-SHA384.		
	STATIC	Ban the use of cipher suites using static keys.		
	CHACHA20	Ban the use of cipher suites using ChaCha20.		
	ARIA	Ban the use of cipher suites using ARIA.		
	AESCCM	Ban the use of cipher suites using AESCCM.		
admin-https-ssl-ciphersuites	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, remove TLS1.3 from admin-https-ssl-versions.	option	-	TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256
	Option	Description		
	TLS-AES-128-GCM-SHA256	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.		
	TLS-AES-256-GCM-SHA384	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.		
	TLS-CHACHA20-POLY1305-SHA256	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.		
	TLS-AES-128-CCM-SHA256	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.		
	TLS-AES-128-CCM-8-SHA256	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.		
admin-https-ssl-versions	Allowed TLS versions for web administration.	option	-	tlsv1-2 tlsv1-3
	Option	Description		
	tlsv1-1	TLS 1.1.		
	tlsv1-2	TLS 1.2.		
	tlsv1-3	TLS 1.3.		

Parameter	Description	Type	Size	Default								
admin-lockout-duration	Amount of time in seconds that an administrator account is locked out after reaching the admin-lockout-threshold for repeated failed login attempts.	integer	Minimum value: 60 1 Maximum value: 2147483647									
admin-lockout-threshold	Number of failed login attempts before an administrator account is locked out for the admin-lockout-duration.	integer	Minimum value: 3 1 Maximum value: 10									
admin-login-max	Maximum number of administrators who can be logged in at the same time (1 - 100, default = 100).	integer	Minimum value: 100 1 Maximum value: 100									
admin-port	Administrative access port for HTTP. (1 - 65535, default = 80).	integer	Minimum value: 80 1 Maximum value: 65535									
admin-reset-button *	Press the reset button can reset to factory default.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>press the reset button can reset to factory default</td></tr><tr><td>disable</td><td>press the reset button cannot reset to factory default</td></tr></table>				Option	Description	enable	press the reset button can reset to factory default	disable	press the reset button cannot reset to factory default		
Option	Description											
enable	press the reset button can reset to factory default											
disable	press the reset button cannot reset to factory default											
admin-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Enable local admin authentication restriction including console.</td></tr><tr><td>non-console-only</td><td>Enable local admin authentication restriction excluding console.</td></tr><tr><td>disable</td><td>Disable local admin authentication restriction.</td></tr></table>				Option	Description	all	Enable local admin authentication restriction including console.	non-console-only	Enable local admin authentication restriction excluding console.	disable	Disable local admin authentication restriction.
Option	Description											
all	Enable local admin authentication restriction including console.											
non-console-only	Enable local admin authentication restriction excluding console.											
disable	Disable local admin authentication restriction.											
admin-scp	Enable/disable SCP support for system configuration backup, restore, and firmware file upload.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SCP support for system configuration backup, restore, and firmware file upload.</td></tr></table>				Option	Description	enable	Enable SCP support for system configuration backup, restore, and firmware file upload.				
Option	Description											
enable	Enable SCP support for system configuration backup, restore, and firmware file upload.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SCP support for system configuration backup, restore, and firmware file upload.</td></tr></table>	Option	Description	<i>disable</i>	Disable SCP support for system configuration backup, restore, and firmware file upload.					
Option	Description									
<i>disable</i>	Disable SCP support for system configuration backup, restore, and firmware file upload.									
admin-server-cert	Server certificate that the FortiGate uses for HTTPS administrative connections.	string	Maximum length: 35	Fortinet_GUI_Server						
admin-sport	Administrative access port for HTTPS. (1 - 65535, default = 443).	integer	Minimum value: 443 1 Maximum value: 65535	443						
admin-ssh-grace-time	Maximum time in seconds permitted between making an SSH connection to the FortiGate unit and authenticating (10 - 3600 sec (1 hour), default 120).	integer	Minimum value: 120 10 Maximum value: 3600	120						
admin-ssh-password	Enable/disable password authentication for SSH admin access.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password authentication for SSH admin access.</td></tr><tr><td><i>disable</i></td><td>Disable password authentication for SSH admin access.</td></tr></table>	Option	Description	<i>enable</i>	Enable password authentication for SSH admin access.	<i>disable</i>	Disable password authentication for SSH admin access.			
Option	Description									
<i>enable</i>	Enable password authentication for SSH admin access.									
<i>disable</i>	Disable password authentication for SSH admin access.									
admin-ssh-port	Administrative access port for SSH. (1 - 65535, default = 22).	integer	Minimum value: 22 1 Maximum value: 65535	22						
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH v1 compatibility.</td></tr><tr><td><i>disable</i></td><td>Disable SSH v1 compatibility.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSH v1 compatibility.	<i>disable</i>	Disable SSH v1 compatibility.			
Option	Description									
<i>enable</i>	Enable SSH v1 compatibility.									
<i>disable</i>	Disable SSH v1 compatibility.									
admin-telnet	Enable/disable TELNET service.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TELNET service.</td></tr><tr><td><i>disable</i></td><td>Disable TELNET service.</td></tr></table>	Option	Description	<i>enable</i>	Enable TELNET service.	<i>disable</i>	Disable TELNET service.			
Option	Description									
<i>enable</i>	Enable TELNET service.									
<i>disable</i>	Disable TELNET service.									

Parameter	Description	Type	Size	Default								
admin-telnet-port	Administrative access port for TELNET. (1 - 65535, default = 23).	integer	Minimum value: 1 Maximum value: 65535	23								
admintimeout	Number of minutes before an idle administrator session times out (1 - 480 minutes (8 hours), default = 5). A shorter idle timeout is more secure.	integer	Minimum value: 1 Maximum value: 480	5								
airplane-mode *	Enable/disable airplane mode.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Shutdown RF signal of internal MODEM and Bluetooth module.</td></tr><tr><td>disable</td><td>Enable RF signal of internal MODEM and Bluetooth module.</td></tr></table>				Option	Description	enable	Shutdown RF signal of internal MODEM and Bluetooth module.	disable	Enable RF signal of internal MODEM and Bluetooth module.		
Option	Description											
enable	Shutdown RF signal of internal MODEM and Bluetooth module.											
disable	Enable RF signal of internal MODEM and Bluetooth module.											
alias	Alias for your FortiGate unit.	string	Maximum length: 35									
allow-traffic-redirect	Disable to prevent traffic with same local ingress and egress interface from being forwarded without policy check.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable allow traffic redirect.</td></tr><tr><td>disable</td><td>Disable allow traffic redirect.</td></tr></table>				Option	Description	enable	Enable allow traffic redirect.	disable	Disable allow traffic redirect.		
Option	Description											
enable	Enable allow traffic redirect.											
disable	Disable allow traffic redirect.											
anti-replay	Level of checking for packet replay and TCP sequence checking.	option	-	strict								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable anti-replay check.</td></tr><tr><td>loose</td><td>Loose anti-replay check.</td></tr><tr><td>strict</td><td>Strict anti-replay check.</td></tr></table>				Option	Description	disable	Disable anti-replay check.	loose	Loose anti-replay check.	strict	Strict anti-replay check.
Option	Description											
disable	Disable anti-replay check.											
loose	Loose anti-replay check.											
strict	Strict anti-replay check.											
application-bandwidth-tracking	Enable/disable application bandwidth tracking.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable application bandwidth tracking.</td></tr><tr><td>enable</td><td>Enable application bandwidth tracking.</td></tr></table>				Option	Description	disable	Disable application bandwidth tracking.	enable	Enable application bandwidth tracking.		
Option	Description											
disable	Disable application bandwidth tracking.											
enable	Enable application bandwidth tracking.											

Parameter	Description	Type	Size	Default						
arp-max-entry	Maximum number of dynamically learned MAC addresses that can be added to the ARP table (131072 - 2147483647, default = 131072).	integer	Minimum value: 131072 Maximum value: 2147483647	131072						
auth-cert	Server certificate that the FortiGate uses for HTTPS firewall authentication connections.	string	Maximum length: 35	Fortinet_Factory						
auth-http-port	User authentication HTTP port. (1 - 65535, default = 1000).	integer	Minimum value: 1 Maximum value: 65535	1000						
auth-https-port	User authentication HTTPS port. (1 - 65535, default = 1003).	integer	Minimum value: 1 Maximum value: 65535	1003						
auth-ike-saml-port	User IKE SAML authentication port (0 - 65535, default = 1001).	integer	Minimum value: 0 Maximum value: 65535	1001						
auth-keepalive	Enable to prevent user authentication sessions from timing out when idle.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of keep alive to extend authentication.</td></tr><tr><td><i>disable</i></td><td>Disable use of keep alive to extend authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of keep alive to extend authentication.	<i>disable</i>	Disable use of keep alive to extend authentication.
Option	Description									
<i>enable</i>	Enable use of keep alive to extend authentication.									
<i>disable</i>	Disable use of keep alive to extend authentication.									
auth-session-auto-backup	Enable/disable automatic and periodic backup of authentication sessions (default = disable). Sessions are restored upon bootup.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable periodic backup of authentication sessions.</td></tr><tr><td><i>disable</i></td><td>Disable periodic backup of authentication sessions.</td></tr></table>				Option	Description	<i>enable</i>	Enable periodic backup of authentication sessions.	<i>disable</i>	Disable periodic backup of authentication sessions.
Option	Description									
<i>enable</i>	Enable periodic backup of authentication sessions.									
<i>disable</i>	Disable periodic backup of authentication sessions.									
auth-session-auto-backup-interval	Configure automatic authentication session backup interval (default = 15min).	option	-	15min						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1min</i></td><td>One minute.</td></tr></table>				Option	Description	<i>1min</i>	One minute.		
Option	Description									
<i>1min</i>	One minute.									

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5min</td><td>Five minutes.</td></tr><tr><td>15min</td><td>Fifteen minutes.</td></tr><tr><td>30min</td><td>Thirty minutes.</td></tr><tr><td>1hr</td><td>One hour.</td></tr></table>	Option	Description	5min	Five minutes.	15min	Fifteen minutes.	30min	Thirty minutes.	1hr	One hour.			
	Option	Description												
	5min	Five minutes.												
	15min	Fifteen minutes.												
	30min	Thirty minutes.												
1hr	One hour.													
auth-session-limit	Action to take when the number of allowed user authenticated sessions is reached.	option	-	block-new										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>block-new</td><td>Block new user authentication attempts.</td></tr><tr><td>logout-inactive</td><td>Logout the most inactive user authenticated sessions.</td></tr></table>	Option	Description	block-new	Block new user authentication attempts.	logout-inactive	Logout the most inactive user authenticated sessions.							
	Option	Description												
	block-new	Block new user authentication attempts.												
logout-inactive	Logout the most inactive user authenticated sessions.													
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension devices.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable automatic authorization of dedicated Fortinet extension device globally.</td></tr><tr><td>disable</td><td>Disable automatic authorization of dedicated Fortinet extension device globally.</td></tr></table>	Option	Description	enable	Enable automatic authorization of dedicated Fortinet extension device globally.	disable	Disable automatic authorization of dedicated Fortinet extension device globally.							
	Option	Description												
	enable	Enable automatic authorization of dedicated Fortinet extension device globally.												
disable	Disable automatic authorization of dedicated Fortinet extension device globally.													
autorun-log-fsck	Enable/disable automatic log partition check after ungraceful shutdown.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable automatic log partition check after ungraceful shutdown.</td></tr><tr><td>disable</td><td>Disable automatic log partition check after ungraceful shutdown.</td></tr></table>	Option	Description	enable	Enable automatic log partition check after ungraceful shutdown.	disable	Disable automatic log partition check after ungraceful shutdown.							
	Option	Description												
	enable	Enable automatic log partition check after ungraceful shutdown.												
disable	Disable automatic log partition check after ungraceful shutdown.													
av-affinity *	Affinity setting for AV scanning (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0										
av-failopen	Set the action to take if the FortiGate is running low on memory or the proxy connection limit has been reached.	option	-	pass										

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.</td></tr><tr><td><i>off</i></td><td>Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.</td></tr><tr><td><i>one-shot</i></td><td>Bypass the antivirus system when memory is low.</td></tr></table>	Option	Description	<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.	<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.	<i>one-shot</i>	Bypass the antivirus system when memory is low.			
	Option	Description										
	<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.										
	<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.										
<i>one-shot</i>	Bypass the antivirus system when memory is low.											
av-failopen-session	When enabled and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by av-failopen.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AV fail open session option.</td></tr><tr><td><i>disable</i></td><td>Disable AV fail open session option.</td></tr></table>	Option	Description	<i>enable</i>	Enable AV fail open session option.	<i>disable</i>	Disable AV fail open session option.					
	Option	Description										
	<i>enable</i>	Enable AV fail open session option.										
<i>disable</i>	Disable AV fail open session option.											
batch-cmdb	Enable/disable batch mode, allowing you to enter a series of CLI commands that will execute as a group once they are loaded.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable batch mode to execute in CMDB server.</td></tr><tr><td><i>disable</i></td><td>Disable batch mode to execute in CMDB server.</td></tr></table>	Option	Description	<i>enable</i>	Enable batch mode to execute in CMDB server.	<i>disable</i>	Disable batch mode to execute in CMDB server.					
	Option	Description										
	<i>enable</i>	Enable batch mode to execute in CMDB server.										
<i>disable</i>	Disable batch mode to execute in CMDB server.											
bfd-affinity	Affinity setting for BFD daemon (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1								
block-session-timer	Duration in seconds for blocked sessions (1 - 300 sec (5 minutes), default = 30).	integer	Minimum value: 1 Maximum value: 300	30								
br-fdb-max-entry	Maximum number of bridge forwarding database (FDB) entries.	integer	Minimum value: 8192 Maximum value: 2147483647	8192								
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647	8								

Parameter	Description	Type	Size	Default								
cfg-revert-timeout	Time-out for reverting to the last saved configuration. (10 - 4294967295 seconds, default = 600).	integer	Minimum value: 10 Maximum value: 4294967295	600								
cfg-save	Configuration file save mode for CLI changes.	option	-	automatic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>automatic</i></td><td>Automatically save config.</td></tr><tr><td><i>manual</i></td><td>Manually save config.</td></tr><tr><td><i>revert</i></td><td>Manually save config and revert the config when timeout.</td></tr></table>	Option	Description	<i>automatic</i>	Automatically save config.	<i>manual</i>	Manually save config.	<i>revert</i>	Manually save config and revert the config when timeout.			
Option	Description											
<i>automatic</i>	Automatically save config.											
<i>manual</i>	Manually save config.											
<i>revert</i>	Manually save config and revert the config when timeout.											
check-protocol-header	Level of checking performed on protocol headers. Strict checking is more thorough but may affect performance. Loose checking is OK in most cases.	option	-	loose								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>loose</i></td><td>Check protocol header loosely.</td></tr><tr><td><i>strict</i></td><td>Check protocol header strictly.</td></tr></table>	Option	Description	<i>loose</i>	Check protocol header loosely.	<i>strict</i>	Check protocol header strictly.					
Option	Description											
<i>loose</i>	Check protocol header loosely.											
<i>strict</i>	Check protocol header strictly.											
check-reset-range	Configure ICMP error message verification. You can either apply strict RST range checking or disable it.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>strict</i></td><td>Check RST range strictly.</td></tr><tr><td><i>disable</i></td><td>Disable RST range check.</td></tr></table>	Option	Description	<i>strict</i>	Check RST range strictly.	<i>disable</i>	Disable RST range check.					
Option	Description											
<i>strict</i>	Check RST range strictly.											
<i>disable</i>	Disable RST range check.											
cli-audit-log	Enable/disable CLI audit log.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable CLI audit log.</td></tr><tr><td><i>disable</i></td><td>Disable CLI audit log.</td></tr></table>	Option	Description	<i>enable</i>	Enable CLI audit log.	<i>disable</i>	Disable CLI audit log.					
Option	Description											
<i>enable</i>	Enable CLI audit log.											
<i>disable</i>	Disable CLI audit log.											
cloud-communication	Enable/disable all cloud communication.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Allow cloud communication.		
	<i>disable</i>	Disable all cloud-related settings.		
clt-cert-req	Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable require client certificate for GUI login.		
	<i>disable</i>	Disable require client certificate for GUI login.		
cmdbsvr-affinity	Affinity setting for cmdbsvr (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	1
cpu-use-threshold	Threshold at which CPU usage is reported (% of total CPU, default = 90).	integer	Minimum value: 50 Maximum value: 99	90
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable CA attribute in CSR.		
	<i>disable</i>	Disable CA attribute in CSR.		
daily-restart	Enable/disable daily restart of FortiGate unit. Use the restart-time option to set the time of day for the restart.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable daily reboot of the FortiGate.		
	<i>disable</i>	Disable daily reboot of the FortiGate.		
default-service-source-port	Default service source port range (default = 1 - 65535).	user	Not Specified	
delay-tcp-npu-session *	Enable TCP NPU session delay to guarantee packet order of 3-way handshake.	option	-	disable

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.</td></tr><tr><td><i>disable</i></td><td>Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.</td></tr></table>	Option	Description	<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.	<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.													
	Option	Description																		
	<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.																		
<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.																			
device-idle-timeout	Time in seconds that a device must be idle to automatically log the device user out. (30 - 31536000 sec (30 sec to 1 year), default = 300).	integer	Minimum value: 30 Maximum value: 31536000	300																
dh-params	Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.	option	-	2048																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1024</td><td>1024 bits.</td></tr><tr><td>1536</td><td>1536 bits.</td></tr><tr><td>2048</td><td>2048 bits.</td></tr><tr><td>3072</td><td>3072 bits.</td></tr><tr><td>4096</td><td>4096 bits.</td></tr><tr><td>6144</td><td>6144 bits.</td></tr><tr><td>8192</td><td>8192 bits.</td></tr></table>	Option	Description	1024	1024 bits.	1536	1536 bits.	2048	2048 bits.	3072	3072 bits.	4096	4096 bits.	6144	6144 bits.	8192	8192 bits.			
	Option	Description																		
	1024	1024 bits.																		
	1536	1536 bits.																		
	2048	2048 bits.																		
	3072	3072 bits.																		
	4096	4096 bits.																		
	6144	6144 bits.																		
8192	8192 bits.																			
dhcp-lease-backup-interval	DHCP leases backup interval in seconds (10 - 3600, default = 60).	integer	Minimum value: 10 Maximum value: 3600	60																
dnsproxy-worker-count	DNS proxy worker count. For a FortiGate with multiple logical CPUs, you can set the DNS process number from 1 to the number of logical CPUs.	integer	Minimum value: 1 Maximum value: 8 **	1																
early-tcp-npu-session	Enable/disable early TCP NPU session.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.</td></tr></table>	Option	Description	<i>enable</i>	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.															
	Option	Description																		
<i>enable</i>	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.																			

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.</td></tr></table>	Option	Description	<i>disable</i>	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.					
Option	Description									
<i>disable</i>	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.									
edit-vdom-prompt *	Enable/disable edit new VDOM prompt.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable edit new VDOM prompt.</td></tr><tr><td><i>disable</i></td><td>Disable edit new VDOM prompt.</td></tr></table>	Option	Description	<i>enable</i>	Enable edit new VDOM prompt.	<i>disable</i>	Disable edit new VDOM prompt.			
Option	Description									
<i>enable</i>	Enable edit new VDOM prompt.									
<i>disable</i>	Disable edit new VDOM prompt.									
extender-controller-reserved-network	Configure reserved network subnet for managed LAN extension FortiExtender units. This is available when the FortiExtender daemon is running.	ipv4-classnet-host	Not Specified	10.252.0.1 255.255.0.0						
failtime	Fail-time for server lost.	integer	Minimum value: 5 0 Maximum value: 4294967295							
faz-disk-buffer-size	Maximum disk buffer size to temporarily store logs destined for FortiAnalyzer. To be used in the event that FortiAnalyzer is unavailable.	integer	Not Specified	0						
fds-statistics	Enable/disable sending IPS, Application Control, and AntiVirus data to FortiGuard. This data is used to improve FortiGuard services and is not shared with external parties and is protected by Fortinet's privacy policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard statistics.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard statistics.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard statistics.	<i>disable</i>	Disable FortiGuard statistics.			
Option	Description									
<i>enable</i>	Enable FortiGuard statistics.									
<i>disable</i>	Disable FortiGuard statistics.									
fds-statistics-period	FortiGuard statistics collection period in minutes. (1 - 1440 min (1 min to 24 hours), default = 60).	integer	Minimum value: 60 1 Maximum value: 1440							
fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-							

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>advisory</i></td><td>Retrieve FortiGuard advisories, report and news alerts.</td></tr><tr><td><i>latest-threat</i></td><td>Retrieve latest FortiGuard threats alerts.</td></tr><tr><td><i>latest-virus</i></td><td>Retrieve latest FortiGuard virus alerts.</td></tr><tr><td><i>latest-attack</i></td><td>Retrieve latest FortiGuard attack alerts.</td></tr><tr><td><i>new-antivirus-db</i></td><td>Retrieve FortiGuard AV database release alerts.</td></tr><tr><td><i>new-attack-db</i></td><td>Retrieve FortiGuard IPS database release alerts.</td></tr></table>	Option	Description	<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.	<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.	<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.	<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.	<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.	<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.			
	Option	Description																
	<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.																
	<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.																
	<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.																
	<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.																
	<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.																
<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.																	
forticontroller-proxy *	Enable/disable FortiController proxy.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.											
	Option	Description																
	<i>enable</i>	Enable setting.																
<i>disable</i>	Disable setting.																	
forticontroller-proxy-port *	FortiController proxy port (1024 - 49150).	integer	Minimum value: 1024 Maximum value: 49150	11133														
forticonverter-config-upload	Enable/disable config upload to FortiConverter.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>once</i></td><td>Enable one-time config upload to FortiConverter.</td></tr><tr><td><i>disable</i></td><td>Disable config upload to FortiConverter.</td></tr></table>	Option	Description	<i>once</i>	Enable one-time config upload to FortiConverter.	<i>disable</i>	Disable config upload to FortiConverter.											
	Option	Description																
	<i>once</i>	Enable one-time config upload to FortiConverter.																
<i>disable</i>	Disable config upload to FortiConverter.																	
forticonverter-integration	Enable/disable FortiConverter integration service.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiConverter integration service.</td></tr><tr><td><i>disable</i></td><td>Disable FortiConverter integration service.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiConverter integration service.	<i>disable</i>	Disable FortiConverter integration service.											
	Option	Description																
	<i>enable</i>	Enable FortiConverter integration service.																
<i>disable</i>	Disable FortiConverter integration service.																	
fortiextender	Enable/disable FortiExtender.	option	-	disable **														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FortiExtender controller.</td></tr><tr><td><i>enable</i></td><td>Enable FortiExtender controller.</td></tr></table>	Option	Description	<i>disable</i>	Disable FortiExtender controller.	<i>enable</i>	Enable FortiExtender controller.											
	Option	Description																
	<i>disable</i>	Disable FortiExtender controller.																
<i>enable</i>	Enable FortiExtender controller.																	

Parameter	Description	Type	Size	Default						
fortiextender-data-port	FortiExtender data port (1024 - 49150, default = 25246).	integer	Minimum value: 1024 Maximum value: 49150	25246						
fortiextender-discovery-lockdown	Enable/disable FortiExtender CAPWAP lockdown.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Unlock down new FortiExtender device discovery.</td></tr><tr><td>enable</td><td>Lock down new FortiExtender device discovery.</td></tr></table>	Option	Description	disable	Unlock down new FortiExtender device discovery.	enable	Lock down new FortiExtender device discovery.			
Option	Description									
disable	Unlock down new FortiExtender device discovery.									
enable	Lock down new FortiExtender device discovery.									
fortiextender-provision-on-authorization	Enable/disable automatic provisioning of latest FortiExtender firmware on authorization.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiExtender firmware provision on authorization.</td></tr><tr><td>disable</td><td>Disable FortiExtender firmware provision on authorization.</td></tr></table>	Option	Description	enable	Enable FortiExtender firmware provision on authorization.	disable	Disable FortiExtender firmware provision on authorization.			
Option	Description									
enable	Enable FortiExtender firmware provision on authorization.									
disable	Disable FortiExtender firmware provision on authorization.									
fortiextender-vlan-mode *	Enable/disable FortiExtender VLAN mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiExtender VLAN mode.</td></tr><tr><td>disable</td><td>Disable FortiExtender VLAN mode.</td></tr></table>	Option	Description	enable	Enable FortiExtender VLAN mode.	disable	Disable FortiExtender VLAN mode.			
Option	Description									
enable	Enable FortiExtender VLAN mode.									
disable	Disable FortiExtender VLAN mode.									
fortigslb-integration	Enable/disable integration with the FortiGSLB cloud service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable VIP and ZTNA server integration with the FortiGSLB cloud service.</td></tr><tr><td>enable</td><td>Enable VIP and ZTNA server integration with the FortiGSLB cloud service.</td></tr></table>	Option	Description	disable	Disable VIP and ZTNA server integration with the FortiGSLB cloud service.	enable	Enable VIP and ZTNA server integration with the FortiGSLB cloud service.			
Option	Description									
disable	Disable VIP and ZTNA server integration with the FortiGSLB cloud service.									
enable	Enable VIP and ZTNA server integration with the FortiGSLB cloud service.									
fortiservice-port	FortiService port (1 - 65535, default = 8013). Used by FortiClient endpoint compliance. Older versions of FortiClient used a different port.	integer	Minimum value: 1 Maximum value: 65535	8013						
fortitoken-cloud	Enable/disable FortiToken Cloud service.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable FortiToken Cloud service.		
	<i>disable</i>	Disable FortiToken Cloud service.		
fortitoken-cloud-push-status	Enable/disable FTM push service of FortiToken Cloud.	option	-	enable
	Option Description			
	<i>enable</i>	Enable FTM push service of FortiToken Cloud.		
	<i>disable</i>	Disable FTM push service of FortiToken Cloud.		
fortitoken-cloud-sync-interval	Interval in which to clean up remote users in FortiToken Cloud (0 - 336 hours (14 days), default = 24, disable = 0).	integer	Minimum value: 0 Maximum value: 336	24
gtpu-dynamic-source-port *	Enable/disable GTP-U dynamic source port support.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
gui-allow-incompatible-fabric-fgt	Enable/disable Allow FGT with incompatible firmware to be treated as compatible in security fabric on the GUI. May cause unexpected error.	option	-	disable
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-app-detection-sdwan	Enable/disable Allow app-detection based SD-WAN.	option	-	disable
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-auto-upgrade-setup-warning	Enable/disable the automatic patch upgrade setup prompt on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-cdn-domain-override	Domain of CDN server.	string	Maximum length: 255	
gui-cdn-usage	Enable/disable Load GUI static files from a CDN.	option	-	disable
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-certificates	Enable/disable the System > Certificate GUI page, allowing you to add and configure certificates from the GUI.	option	-	enable **
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-custom-language	Enable/disable custom languages in GUI.	option	-	disable
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-date-format	Default date format used throughout GUI.	option	-	yyyy/MM/dd
	Option Description			
	<i>yyyy/MM/dd</i>	Year/Month/Day.		
	<i>dd/MM/yyyy</i>	Day/Month/Year.		
	<i>MM/dd/yyyy</i>	Month/Day/Year.		
	<i>yyyy-MM-dd</i>	Year-Month-Day.		
	<i>dd-MM-yyyy</i>	Day-Month-Year.		
	<i>MM-dd-yyyy</i>	Month-Day-Year.		

Parameter	Description	Type	Size	Default						
gui-date-time-source	Source from which the FortiGate GUI uses to display date and time entries.	option	-	system						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>system</td><td>Use this FortiGate unit's configured timezone.</td></tr><tr><td>browser</td><td>Use the web browser's timezone.</td></tr></table>	Option	Description	system	Use this FortiGate unit's configured timezone.	browser	Use the web browser's timezone.			
Option	Description									
system	Use this FortiGate unit's configured timezone.									
browser	Use the web browser's timezone.									
gui-device-latitude	Add the latitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19							
gui-device-longitude	Add the longitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19							
gui-display-hostname	Enable/disable displaying the FortiGate's hostname on the GUI login page.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Display the feature in GUI.</td></tr><tr><td>disable</td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	enable	Display the feature in GUI.	disable	Do not display the feature in GUI.			
Option	Description									
enable	Display the feature in GUI.									
disable	Do not display the feature in GUI.									
gui-firmware-upgrade-warning	Enable/disable the firmware upgrade warning on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Display the feature in GUI.</td></tr><tr><td>disable</td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	enable	Display the feature in GUI.	disable	Do not display the feature in GUI.			
Option	Description									
enable	Display the feature in GUI.									
disable	Do not display the feature in GUI.									
gui-forticare-registration-setup-warning	Enable/disable the FortiCare registration setup warning on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Display the feature in GUI.</td></tr><tr><td>disable</td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	enable	Display the feature in GUI.	disable	Do not display the feature in GUI.			
Option	Description									
enable	Display the feature in GUI.									
disable	Do not display the feature in GUI.									
gui-fortigate-cloud-sandbox	Enable/disable displaying FortiGate Cloud Sandbox on the GUI.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-local-out	Enable/disable Local-out traffic on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-replacement-message-groups	Enable/disable replacement message groups on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-rest-api-cache *	Enable/disable REST API result caching on FortiGate.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable REST API result caching on FortiGate.		
	<i>disable</i>	Disable REST API result caching on FortiGate.		
gui-theme	Color scheme for the administration GUI.	option	-	jade
	Option	Description		
	<i>jade</i>	Jade theme.		
	<i>neutrino</i>	Neutrino theme.		
	<i>mariner</i>	Mariner theme.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>graphite</i></td><td>Graphite theme.</td></tr><tr><td><i>melongene</i></td><td>Melongene theme.</td></tr><tr><td><i>jet-stream</i></td><td>Jet Stream theme.</td></tr><tr><td><i>security-fabric</i></td><td>Security Fabric theme.</td></tr><tr><td><i>retro</i></td><td>FortiOS v3 Retro theme.</td></tr><tr><td><i>dark-matter</i></td><td>Dark Matter theme.</td></tr><tr><td><i>onyx</i></td><td>Onyx theme.</td></tr><tr><td><i>eclipse</i></td><td>Eclipse theme.</td></tr></table>	Option	Description	<i>graphite</i>	Graphite theme.	<i>melongene</i>	Melongene theme.	<i>jet-stream</i>	Jet Stream theme.	<i>security-fabric</i>	Security Fabric theme.	<i>retro</i>	FortiOS v3 Retro theme.	<i>dark-matter</i>	Dark Matter theme.	<i>onyx</i>	Onyx theme.	<i>eclipse</i>	Eclipse theme.			
	Option	Description																				
	<i>graphite</i>	Graphite theme.																				
	<i>melongene</i>	Melongene theme.																				
	<i>jet-stream</i>	Jet Stream theme.																				
	<i>security-fabric</i>	Security Fabric theme.																				
	<i>retro</i>	FortiOS v3 Retro theme.																				
	<i>dark-matter</i>	Dark Matter theme.																				
	<i>onyx</i>	Onyx theme.																				
<i>eclipse</i>	Eclipse theme.																					
gui-wireless-opensecurity	Enable/disable wireless open security option on the GUI.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display the feature in GUI.</td></tr><tr><td><i>disable</i></td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.															
	Option	Description																				
	<i>enable</i>	Display the feature in GUI.																				
<i>disable</i>	Do not display the feature in GUI.																					
gui-workflow-management	Enable/disable Workflow management features on the GUI.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display the feature in GUI.</td></tr><tr><td><i>disable</i></td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.															
	Option	Description																				
	<i>enable</i>	Display the feature in GUI.																				
<i>disable</i>	Do not display the feature in GUI.																					
ha-affinity	Affinity setting for HA daemons (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1																		
honor-df	Enable/disable honoring of Don't-Fragment (DF) flag.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable honoring of Don't-Fragment flag.</td></tr><tr><td><i>disable</i></td><td>Disable honoring of Don't-Fragment flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable honoring of Don't-Fragment flag.	<i>disable</i>	Disable honoring of Don't-Fragment flag.															
	Option	Description																				
	<i>enable</i>	Enable honoring of Don't-Fragment flag.																				
<i>disable</i>	Disable honoring of Don't-Fragment flag.																					

Parameter	Description	Type	Size	Default										
hostname	FortiGate unit's hostname. Most models will truncate names longer than 24 characters. Some models support hostnames up to 35 characters.	string	Maximum length: 35											
httpd-max-worker-count	Maximum number of simultaneous HTTP requests that will be served. This number may affect GUI and REST API performance (0 - 128, default = 0 means let system decide).	integer	Minimum value: 0 Maximum value: 128											
hyper-scale-vdom-num *	Number of VDOMs for hyper scale license.	integer	Minimum value: 250 Maximum value: 250											
igmp-state-limit	Maximum number of IGMP memberships (96 - 64000, default = 3200).	integer	Minimum value: 96 Maximum value: 128000											
interface-subnet-usage	Enable/disable allowing use of interface-subnet setting in firewall addresses (default = enable).	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disallow use of the interface-subnet setting in firewall addresses. Use in conjunction with the FortiGate REST API and when a large number of firewall addresses exist in the configuration.</td></tr><tr><td>enable</td><td>Allow use of the interface-subnet setting in firewall addresses.</td></tr></table>				Option	Description	disable	Disallow use of the interface-subnet setting in firewall addresses. Use in conjunction with the FortiGate REST API and when a large number of firewall addresses exist in the configuration.	enable	Allow use of the interface-subnet setting in firewall addresses.				
Option	Description													
disable	Disallow use of the interface-subnet setting in firewall addresses. Use in conjunction with the FortiGate REST API and when a large number of firewall addresses exist in the configuration.													
enable	Allow use of the interface-subnet setting in firewall addresses.													
internet-service-database	Configure which Internet Service database size to download from FortiGuard and use.	option	-	full **										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mini</td><td>Small sized Internet Service database with very limited IP addresses.</td></tr><tr><td>standard</td><td>Medium sized Internet Service database with most IP addresses.</td></tr><tr><td>full</td><td>Full sized Internet Service database with all IP addresses.</td></tr><tr><td>on-demand</td><td>Internet Service database with customer selected IP addresses.</td></tr></table>				Option	Description	mini	Small sized Internet Service database with very limited IP addresses.	standard	Medium sized Internet Service database with most IP addresses.	full	Full sized Internet Service database with all IP addresses.	on-demand	Internet Service database with customer selected IP addresses.
Option	Description													
mini	Small sized Internet Service database with very limited IP addresses.													
standard	Medium sized Internet Service database with most IP addresses.													
full	Full sized Internet Service database with all IP addresses.													
on-demand	Internet Service database with customer selected IP addresses.													
internet-service-download-list <id>	Configure which on-demand Internet Service IDs are to be downloaded. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295											

Parameter	Description	Type	Size	Default						
interval	Dead gateway detection interval.	integer	Minimum value: 0 Maximum value: 4294967295	5						
ip-conflict-detection	Enable/disable logging of IPv4 address conflict detection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging of IPv4 address conflict detection.</td></tr><tr><td>disable</td><td>Disable logging of IPv4 address conflict detection.</td></tr></table>	Option	Description	enable	Enable logging of IPv4 address conflict detection.	disable	Disable logging of IPv4 address conflict detection.			
Option	Description									
enable	Enable logging of IPv4 address conflict detection.									
disable	Disable logging of IPv4 address conflict detection.									
ip-fragment-mem-thresholds	Maximum memory (MB) used to reassemble IPv4/IPv6 fragments.	integer	Minimum value: 32 Maximum value: 2047	32						
ip-fragment-timeout	Timeout value in seconds for any fragment not being reassembled	integer	Minimum value: 3 Maximum value: 30	30						
ip-src-port-range	IP source port range used for traffic originating from the FortiGate unit.	user	Not Specified	1024-25000						
ips-affinity *	Affinity setting for IPS (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons).	string	Maximum length: 79	0						
ipsec-asic-offload *	Enable/disable ASIC offloading (hardware acceleration) for IPsec VPN traffic. Hardware acceleration can offload IPsec VPN sessions and accelerate encryption and decryption.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ASIC offload for IPsec VPN.</td></tr><tr><td>disable</td><td>Disable ASIC offload for IPsec VPN.</td></tr></table>	Option	Description	enable	Enable ASIC offload for IPsec VPN.	disable	Disable ASIC offload for IPsec VPN.			
Option	Description									
enable	Enable ASIC offload for IPsec VPN.									
disable	Disable ASIC offload for IPsec VPN.									
ipsec-ha-seqjump-rate	ESP jump ahead rate (1G - 10G pps equivalent).	integer	Minimum value: 1 Maximum value: 10	10						
ipsec-hmac-offload *	Enable/disable offloading (hardware acceleration) of HMAC processing for IPsec VPN.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable offload IPsec HMAC processing to hardware if possible.		
	<i>disable</i>	Disable offload IPsec HMAC processing to hardware.		
ipsec-qat-offload *	Enable/disable QAT offloading (Intel QuickAssist) for IPsec VPN traffic. QuickAssist can accelerate IPsec encryption and decryption.	option	-	enable
	Option Description			
	<i>enable</i>	Enable QAT offload for IPsec VPN.		
	<i>disable</i>	Disable QAT offload for IPsec VPN.		
ipv6-accept-dad	Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD).	integer	Minimum value: 1 0 Maximum value: 2	
ipv6-allow-anycast-probe	Enable/disable IPv6 address probe through Anycast.	option	-	disable
	Option Description			
	<i>enable</i>	Enable probing of IPv6 address space through Anycast		
	<i>disable</i>	Disable probing of IPv6 address space through Anycast		
ipv6-allow-local-in-silent-drop	Enable/disable silent drop of IPv6 local-in traffic.	option	-	enable
	Option Description			
	<i>enable</i>	Enable silent drop of IPv6 local-in traffic.		
	<i>disable</i>	Disable silent drop of IPv6 local-in traffic.		
ipv6-allow-multicast-probe	Enable/disable IPv6 address probe through Multicast.	option	-	disable
	Option Description			
	<i>enable</i>	Enable probing of IPv6 address space through Multicast.		
	<i>disable</i>	Disable probing of IPv6 address space through Multicast.		
ipv6-allow-traffic-redirect	Disable to prevent IPv6 traffic with same local ingress and egress interface from being forwarded without policy check.	option	-	enable

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allow traffic IPv6 redirect.</td></tr><tr><td><i>disable</i></td><td>Disable allow traffic IPv6 redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable allow traffic IPv6 redirect.	<i>disable</i>	Disable allow traffic IPv6 redirect.															
	Option	Description																				
	<i>enable</i>	Enable allow traffic IPv6 redirect.																				
<i>disable</i>	Disable allow traffic IPv6 redirect.																					
ipv6-fragment-timeout	Timeout value in seconds for any IPv6 fragment not being reassembled	integer	Minimum value: 60 5 Maximum value: 60	60																		
irq-time-accounting	Configure CPU IRQ time accounting mode.	option	-	auto																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically switch CPU accounting mode.</td></tr><tr><td><i>force</i></td><td>Force the use of CPU IRQ time accounting mode.</td></tr></table>	Option	Description	<i>auto</i>	Automatically switch CPU accounting mode.	<i>force</i>	Force the use of CPU IRQ time accounting mode.															
	Option	Description																				
	<i>auto</i>	Automatically switch CPU accounting mode.																				
<i>force</i>	Force the use of CPU IRQ time accounting mode.																					
language	GUI display language.	option	-	english																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>english</i></td><td>English.</td></tr><tr><td><i>french</i></td><td>French.</td></tr><tr><td><i>spanish</i></td><td>Spanish.</td></tr><tr><td><i>portuguese</i></td><td>Portuguese.</td></tr><tr><td><i>japanese</i></td><td>Japanese.</td></tr><tr><td><i>trach</i></td><td>Traditional Chinese.</td></tr><tr><td><i>simch</i></td><td>Simplified Chinese.</td></tr><tr><td><i>korean</i></td><td>Korean.</td></tr></table>	Option	Description	<i>english</i>	English.	<i>french</i>	French.	<i>spanish</i>	Spanish.	<i>portuguese</i>	Portuguese.	<i>japanese</i>	Japanese.	<i>trach</i>	Traditional Chinese.	<i>simch</i>	Simplified Chinese.	<i>korean</i>	Korean.			
	Option	Description																				
	<i>english</i>	English.																				
	<i>french</i>	French.																				
	<i>spanish</i>	Spanish.																				
	<i>portuguese</i>	Portuguese.																				
	<i>japanese</i>	Japanese.																				
	<i>trach</i>	Traditional Chinese.																				
<i>simch</i>	Simplified Chinese.																					
<i>korean</i>	Korean.																					
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds (1 - 300000, default 500).	integer	Minimum value: 500 1 Maximum value: 300000	500																		
legacy-poe-device-support *	Enable/disable legacy POE device support.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable legacy POE device support.</td></tr><tr><td><i>disable</i></td><td>Disable legacy POE device support.</td></tr></table>	Option	Description	<i>enable</i>	Enable legacy POE device support.	<i>disable</i>	Disable legacy POE device support.															
	Option	Description																				
	<i>enable</i>	Enable legacy POE device support.																				
<i>disable</i>	Disable legacy POE device support.																					

Parameter	Description	Type	Size	Default						
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reception of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td><i>disable</i></td><td>Disable reception of Link Layer Discovery Protocol (LLDP).</td></tr></table>	Option	Description	<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).	<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).			
Option	Description									
<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).									
<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).									
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable transmission of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td><i>disable</i></td><td>Disable transmission of Link Layer Discovery Protocol (LLDP).</td></tr></table>	Option	Description	<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).	<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).			
Option	Description									
<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).									
<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).									
log-single-cpu-high	Enable/disable logging the event of a single CPU core reaching CPU usage threshold.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging the event of a single CPU core reaching CPU usage threshold.</td></tr><tr><td><i>disable</i></td><td>Disable logging the event of a single CPU core reaching CPU usage threshold.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging the event of a single CPU core reaching CPU usage threshold.	<i>disable</i>	Disable logging the event of a single CPU core reaching CPU usage threshold.			
Option	Description									
<i>enable</i>	Enable logging the event of a single CPU core reaching CPU usage threshold.									
<i>disable</i>	Disable logging the event of a single CPU core reaching CPU usage threshold.									
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging of SSL connection events.</td></tr><tr><td><i>disable</i></td><td>Disable logging of SSL connection events.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging of SSL connection events.	<i>disable</i>	Disable logging of SSL connection events.			
Option	Description									
<i>enable</i>	Enable logging of SSL connection events.									
<i>disable</i>	Disable logging of SSL connection events.									
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable insertion of address UUID to traffic logs.</td></tr><tr><td><i>disable</i></td><td>Disable insertion of address UUID to traffic logs.</td></tr></table>	Option	Description	<i>enable</i>	Enable insertion of address UUID to traffic logs.	<i>disable</i>	Disable insertion of address UUID to traffic logs.			
Option	Description									
<i>enable</i>	Enable insertion of address UUID to traffic logs.									
<i>disable</i>	Disable insertion of address UUID to traffic logs.									
login-timestamp	Enable/disable login time recording.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable login time recording.		
	<i>disable</i>	Disable login time recording.		
long-vdom-name *	Enable/disable long VDOM name support.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable long VDOM name support.		
	<i>disable</i>	Disable long VDOM name support.		
management-ip	Management IP address of this FortiGate. Used to log into this FortiGate from another FortiGate in the Security Fabric.	string	Maximum length: 255	
management-port	Overriding port for management connection (Overrides admin port).	integer	Minimum value: 443 1 Maximum value: 65535	
management-port-use-admin-sport	Enable/disable use of the admin-sport setting for the management port. If disabled, FortiGate will allow user to specify management-port.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of the admin-sport setting for the management port.		
	<i>disable</i>	Disable use of the admin-sport setting for the management port.		
management-vdom	Management virtual domain name.	string	Maximum length: 31	root
max-route-cache-size	Maximum number of IP route cache entries (0 - 2147483647).	integer	Minimum value: 0 0 Maximum value: 2147483647	
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme (new sessions are dropped) (% of total RAM, default = 95).	integer	Minimum value: 70 70 Maximum value: 97	95
memory-use-threshold-green	Threshold at which memory usage forces the FortiGate to exit conserve mode (% of total RAM, default = 82).	integer	Minimum value: 70 70 Maximum value: 97	82

Parameter	Description	Type	Size	Default						
memory-use-threshold-red	Threshold at which memory usage forces the FortiGate to enter conserve mode (% of total RAM, default = 88).	integer	Minimum value: 70 Maximum value: 97	88						
miglog-affinity *	Affinity setting for logging (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0						
miglogd-children	Number of logging (miglogd) processes to be allowed to run. Higher number can reduce performance; lower number can slow log processing time.	integer	Minimum value: 0 Maximum value: 15	0						
multi-factor-authentication	Enforce all login methods to require an additional authentication factor (default = optional).	option	-	optional						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>optional</i></td><td>Do not enforce all login methods to require an additional authentication factor (controlled by user settings).</td></tr><tr><td><i>mandatory</i></td><td>Enforce all login methods to require an additional authentication factor.</td></tr></table>				Option	Description	<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).	<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.
Option	Description									
<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).									
<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.									
ndp-max-entry	Maximum number of NDP table entries (set to 65,536 or higher; if set to 0, kernel holds 65,536 entries).	integer	Minimum value: 65536 Maximum value: 2147483647	0						
npu-neighbor-update *	Enable/disable sending of ARP/ICMP6 probing packets to update neighbors for offloaded sessions.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of ARP/ICMP6 probing packets to update neighbors for offloaded sessions.</td></tr><tr><td><i>disable</i></td><td>Disable sending of ARP/ICMP6 probing packets to update neighbors for offloaded sessions.</td></tr></table>				Option	Description	<i>enable</i>	Enable sending of ARP/ICMP6 probing packets to update neighbors for offloaded sessions.	<i>disable</i>	Disable sending of ARP/ICMP6 probing packets to update neighbors for offloaded sessions.
Option	Description									
<i>enable</i>	Enable sending of ARP/ICMP6 probing packets to update neighbors for offloaded sessions.									
<i>disable</i>	Disable sending of ARP/ICMP6 probing packets to update neighbors for offloaded sessions.									
per-user-bal *	Enable/disable per-user block/allow list filter.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable per-user block/allow list filter.		
	<i>disable</i>	Disable per-user block/allow list filter.		
pmtu-discovery	Enable/disable path MTU discovery.	option	-	disable
	Option Description			
	<i>enable</i>	Enable path MTU discovery.		
	<i>disable</i>	Disable path MTU discovery.		
policy-auth-concurrent	Number of concurrent firewall use logins from the same user (1 - 100, default = 0 means no limit).	integer	Minimum value: 0 0 Maximum value: 100	
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-	disable
	Option Description			
	<i>disable</i>	Disable post-login banner.		
	<i>enable</i>	Enable post-login banner.		
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-	disable
	Option Description			
	<i>enable</i>	Enable pre-login banner.		
	<i>disable</i>	Disable pre-login banner.		
private-data-encryption	Enable/disable private data encryption using an AES 128-bit key or passphrase.	option	-	disable
	Option Description			
	<i>disable</i>	Disable private data encryption using an AES 128-bit key.		
	<i>enable</i>	Enable private data encryption using an AES 128-bit key.		

Parameter	Description	Type	Size	Default						
proxy-auth-lifetime	Enable/disable authenticated users lifetime control. This is a cap on the total time a proxy user can be authenticated for after which re-authentication will take place.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authenticated users lifetime control.</td></tr><tr><td><i>disable</i></td><td>Disable authenticated users lifetime control.</td></tr></table>	Option	Description	<i>enable</i>	Enable authenticated users lifetime control.	<i>disable</i>	Disable authenticated users lifetime control.			
Option	Description									
<i>enable</i>	Enable authenticated users lifetime control.									
<i>disable</i>	Disable authenticated users lifetime control.									
proxy-auth-lifetime-timeout	Lifetime timeout in minutes for authenticated users (5 - 65535 min, default=480 (8 hours)).	integer	Minimum value: 5 Maximum value: 65535	480						
proxy-auth-timeout	Authentication timeout in minutes for authenticated users (1 - 10000 min, default = 10).	integer	Minimum value: 1 Maximum value: 10000	10						
proxy-cert-use-mgmt-vdom	Enable/disable using management VDOM to send requests.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-hardware-acceleration *	Enable/disable email proxy hardware acceleration.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable email proxy hardware acceleration.</td></tr><tr><td><i>enable</i></td><td>Enable email proxy hardware acceleration.</td></tr></table>	Option	Description	<i>disable</i>	Disable email proxy hardware acceleration.	<i>enable</i>	Enable email proxy hardware acceleration.			
Option	Description									
<i>disable</i>	Disable email proxy hardware acceleration.									
<i>enable</i>	Enable email proxy hardware acceleration.									
proxy-keep-alive-mode	Control if users must re-authenticate after a session is closed, traffic has been idle, or from the point at which the user was authenticated.	option	-	session						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>session</i></td><td>Proxy keep-alive timeout begins at the closure of the session.</td></tr><tr><td><i>traffic</i></td><td>Proxy keep-alive timeout begins after traffic has not been received.</td></tr></table>	Option	Description	<i>session</i>	Proxy keep-alive timeout begins at the closure of the session.	<i>traffic</i>	Proxy keep-alive timeout begins after traffic has not been received.			
Option	Description									
<i>session</i>	Proxy keep-alive timeout begins at the closure of the session.									
<i>traffic</i>	Proxy keep-alive timeout begins after traffic has not been received.									

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>re-authentication</i></td><td>Proxy keep-alive timeout begins when the user was authenticated.</td></tr></table>				Option	Description	<i>re-authentication</i>	Proxy keep-alive timeout begins when the user was authenticated.																
	Option	Description																						
<i>re-authentication</i>	Proxy keep-alive timeout begins when the user was authenticated.																							
proxy-re-authentication-time	The time limit that users must re-authenticate if proxy-keep-alive-mode is set to re-authenticate (1 - 86400 sec, default=30s.	integer	Minimum value: 30 1 Maximum value: 86400																					
proxy-resource-mode	Enable/disable use of the maximum memory usage on the FortiGate unit's proxy processing of resources, such as block lists, allow lists, and external resources.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of the maximum memory usage.</td></tr><tr><td><i>disable</i></td><td>Disable use of the maximum memory usage.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of the maximum memory usage.	<i>disable</i>	Disable use of the maximum memory usage.														
	Option	Description																						
	<i>enable</i>	Enable use of the maximum memory usage.																						
<i>disable</i>	Disable use of the maximum memory usage.																							
proxy-worker-count *	Proxy worker count.	integer	Minimum value: 0 1 Maximum value: 8 **																					
purdue-level	Purdue Level of this FortiGate.	option	-	3																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Level 1 - Basic Control</td></tr><tr><td>1.5</td><td>Level 1.5</td></tr><tr><td>2</td><td>Level 2 - Area Supervisory Control</td></tr><tr><td>2.5</td><td>Level 2.5</td></tr><tr><td>3</td><td>Level 3 - Operations & Control</td></tr><tr><td>3.5</td><td>Level 3.5</td></tr><tr><td>4</td><td>Level 4 - Business Planning & Logistics</td></tr><tr><td>5</td><td>Level 5 - Enterprise Network</td></tr><tr><td>5.5</td><td>Level 5.5</td></tr></table>				Option	Description	1	Level 1 - Basic Control	1.5	Level 1.5	2	Level 2 - Area Supervisory Control	2.5	Level 2.5	3	Level 3 - Operations & Control	3.5	Level 3.5	4	Level 4 - Business Planning & Logistics	5	Level 5 - Enterprise Network	5.5	Level 5.5
	Option	Description																						
	1	Level 1 - Basic Control																						
	1.5	Level 1.5																						
	2	Level 2 - Area Supervisory Control																						
	2.5	Level 2.5																						
	3	Level 3 - Operations & Control																						
	3.5	Level 3.5																						
	4	Level 4 - Business Planning & Logistics																						
	5	Level 5 - Enterprise Network																						
5.5	Level 5.5																							
quic-ack-threshold	Maximum number of unacknowledged packets before sending ACK (2 - 5, default = 3).	integer	Minimum value: 3 2 Maximum value: 5																					

Parameter	Description	Type	Size	Default
quic-congestion-control-algo	QUIC congestion control algorithm (default = cubic).	option	-	cubic
	Option Description			
	<i>cubic</i>	Cubic.		
	<i>bbr</i>	BBR.		
	<i>bbr2</i>	BBR2.		
	<i>reno</i>	Reno.		
quic-max-datagram-size	Maximum transmit datagram size (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500
quic-pmtud	Enable/disable path MTU discovery (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable path MTU discovery.		
	<i>disable</i>	Disable path MTU discovery.		
quic-tls-handshake-timeout	Time-to-live (TTL) for TLS handshake in seconds (1 - 60, default = 5).	integer	Minimum value: 1 Maximum value: 60	5
quic-udp-payload-size-shaping-per-cid	Enable/disable UDP payload size shaping per connection ID (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable UDP payload size shaping per connection ID.		
	<i>disable</i>	Disable UDP payload size shaping per connection ID.		
radius-port	RADIUS service port number.	integer	Minimum value: 1 Maximum value: 65535	1812
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-	enable
	Option Description			
	<i>enable</i>	Enable reboot of system upon restoring configuration.		
	<i>disable</i>	Disable reboot of system upon restoring configuration.		

Parameter	Description	Type	Size	Default						
refresh	Statistics refresh interval second(s) in GUI.	integer	Minimum value: 0 0 Maximum value: 4294967295							
remoteauthtimeout	Number of seconds that the FortiGate waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. (1-300 sec, default = 5).	integer	Minimum value: 5 1 Maximum value: 300							
reset-sessionless-tcp	Action to perform if the FortiGate receives a TCP packet but cannot find a corresponding session in its session table. NAT/Route mode only.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reset session-less TCP.</td></tr><tr><td>disable</td><td>Disable reset session-less TCP.</td></tr></table>				Option	Description	enable	Enable reset session-less TCP.	disable	Disable reset session-less TCP.
Option	Description									
enable	Enable reset session-less TCP.									
disable	Disable reset session-less TCP.									
rest-api-key-url-query	Enable/disable support for passing REST API keys through URL query parameters.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable support for passing REST API keys through URL query parameters.</td></tr><tr><td>disable</td><td>Disable support for passing REST API keys through URL query parameters.</td></tr></table>				Option	Description	enable	Enable support for passing REST API keys through URL query parameters.	disable	Disable support for passing REST API keys through URL query parameters.
Option	Description									
enable	Enable support for passing REST API keys through URL query parameters.									
disable	Disable support for passing REST API keys through URL query parameters.									
restart-time	Daily restart time (hh:mm).	user	Not Specified							
revision-backup-on-logout	Enable/disable back-up of the latest configuration revision when an administrator logs out of the CLI or GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable revision config backup automatically when logout.</td></tr><tr><td>disable</td><td>Disable revision config backup automatically when logout.</td></tr></table>				Option	Description	enable	Enable revision config backup automatically when logout.	disable	Disable revision config backup automatically when logout.
Option	Description									
enable	Enable revision config backup automatically when logout.									
disable	Disable revision config backup automatically when logout.									
revision-image-auto-backup	Enable/disable back-up of the latest image revision after the firmware is upgraded.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable revision image backup automatically when upgrading image.		
	<i>disable</i>	Disable revision image backup automatically when upgrading image.		
scanunit-count	Number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiGate units with multiple CPUs.	integer	Minimum value: 0 1 Maximum value: 8 **	
scim-http-port	SCIM http port (0 - 65535, default = 44558).	integer	Minimum value: 44558 0 Maximum value: 65535	
scim-https-port	SCIM port (0 - 65535, default = 44559).	integer	Minimum value: 44559 0 Maximum value: 65535	
scim-server-cert	Server certificate that the FortiGate uses for SCIM connections.	string	Maximum length: 35	Fortinet_Factory
send-pmtu-icmp	Enable/disable sending of path maximum transmission unit (PMTU) - ICMP destination unreachable packet and to support PMTUD protocol on your network to reduce fragmentation of packets.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sending of PMTU ICMP destination unreachable packet.		
	<i>disable</i>	Disable sending of PMTU ICMP destination unreachable packet.		
sflowd-max-children-num	Maximum number of sflowd child processes allowed to run.	integer	Minimum value: 6 ** 0 Maximum value: 6 **	
show-backplane-intf *	show/hide backplane interfaces	option	-	disable
	Option	Description		
	<i>enable</i>	show backplane interfaces		
	<i>disable</i>	hide backplane interfaces		
single-vdom-npuvlink *	Enable/disable NPU VDOMs links for single VDOM.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable NPU VDOM links for single VDOM.		
	<i>disable</i>	Disable NPU VDOM links for single VDOM.		
snat-route-change	Enable/disable the ability to change the source NAT route.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SNAT route change.		
	<i>disable</i>	Disable SNAT route change.		
special-file-23-support	Enable/disable detection of those special format files when using Data Loss Prevention.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable detection of those special format files when using Data Loss Prevention.		
	<i>enable</i>	Enable detection of those special format files when using Data Loss Prevention.		
speedtest-server	Enable/disable speed test server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable speed test server service.		
	<i>disable</i>	Disable speed test server service.		
speedtestd-ctrl-port	Speedtest server controller port number.	integer	Minimum value: 5200 1 Maximum value: 65535	
speedtestd-server-port	Speedtest server port number.	integer	Minimum value: 5201 1 Maximum value: 65535	
split-port *	Split port(s) to multiple 10Gbps ports.	string	Maximum length: 15	
ssd-trim-date *	Date within a month to run ssd trim.	integer	Minimum value: 1 1 Maximum value: 31	

Parameter	Description	Type	Size	Default																
ssd-trim-freq *	How often to run SSD Trim (default = weekly). SSD Trim prevents SSD drive data loss by finding and isolating errors.	option	-	weekly																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>never</td><td>Never Run SSD Trim.</td></tr><tr><td>hourly</td><td>Run SSD Trim Hourly.</td></tr><tr><td>daily</td><td>Run SSD Trim Daily.</td></tr><tr><td>weekly</td><td>Run SSD Trim Weekly.</td></tr><tr><td>monthly</td><td>Run SSD Trim Monthly.</td></tr></table>	Option	Description	never	Never Run SSD Trim.	hourly	Run SSD Trim Hourly.	daily	Run SSD Trim Daily.	weekly	Run SSD Trim Weekly.	monthly	Run SSD Trim Monthly.							
Option	Description																			
never	Never Run SSD Trim.																			
hourly	Run SSD Trim Hourly.																			
daily	Run SSD Trim Daily.																			
weekly	Run SSD Trim Weekly.																			
monthly	Run SSD Trim Monthly.																			
ssd-trim-hour *	Hour of the day on which to run SSD Trim (0 - 23, default = 1).	integer	Minimum value: 1 0 Maximum value: 23																	
ssd-trim-min *	Minute of the hour on which to run SSD Trim (0 - 59, 60 for random).	integer	Minimum value: 60 0 Maximum value: 60																	
ssd-trim-weekday *	Day of week to run SSD Trim.	option	-	sunday																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sunday</td><td>Sunday</td></tr><tr><td>monday</td><td>Monday</td></tr><tr><td>tuesday</td><td>Tuesday</td></tr><tr><td>wednesday</td><td>Wednesday</td></tr><tr><td>thursday</td><td>Thursday</td></tr><tr><td>friday</td><td>Friday</td></tr><tr><td>saturday</td><td>Saturday</td></tr></table>	Option	Description	sunday	Sunday	monday	Monday	tuesday	Tuesday	wednesday	Wednesday	thursday	Thursday	friday	Friday	saturday	Saturday			
Option	Description																			
sunday	Sunday																			
monday	Monday																			
tuesday	Tuesday																			
wednesday	Wednesday																			
thursday	Thursday																			
friday	Friday																			
saturday	Saturday																			
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default = TLSv1.2).	option	-	TLSv1-2																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr></table>	Option	Description	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.											
Option	Description																			
SSLv3	SSLv3.																			
TLSv1	TLSv1.																			
TLSv1-1	TLSv1.1.																			

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLsv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLsv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	TLsv1-2	TLSv1.2.	TLsv1-3	TLSv1.3.			
	Option	Description								
	TLsv1-2	TLSv1.2.								
TLsv1-3	TLSv1.3.									
ssl-static-key-ciphers	Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable static key ciphers in SSL/TLS connections.</td></tr><tr><td>disable</td><td>Disable static key ciphers in SSL/TLS connections.</td></tr></table>	Option	Description	enable	Enable static key ciphers in SSL/TLS connections.	disable	Disable static key ciphers in SSL/TLS connections.			
	Option	Description								
	enable	Enable static key ciphers in SSL/TLS connections.								
disable	Disable static key ciphers in SSL/TLS connections.									
sslvpn-affinity *	Agentless VPN CPU affinity.	string	Maximum length: 79	0						
sslvpn-max-worker-count *	Maximum number of Agentless VPN processes. Upper limit for this value is the number of CPUs and depends on the model. Default value of zero means the sslvpnd daemon decides the number of worker processes.	integer	Minimum value: 0 Maximum value: 7 **	0						
sslvpn-web-mode *	Enable/disable Agentless VPN web mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Agentless VPN web mode.</td></tr><tr><td>disable</td><td>Disable Agentless VPN web mode.</td></tr></table>	Option	Description	enable	Enable Agentless VPN web mode.	disable	Disable Agentless VPN web mode.			
	Option	Description								
	enable	Enable Agentless VPN web mode.								
disable	Disable Agentless VPN web mode.									
strict-dirty-session-check	Enable to check the session against the original policy when revalidating. This can prevent dropping of redirected sessions when web-filtering and authentication are enabled together. If this option is enabled, the FortiGate unit deletes a session if a routing or policy change causes the session to no longer match the policy that originally allowed the session.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict dirty-session check.</td></tr><tr><td><i>disable</i></td><td>Disable strict dirty-session check.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict dirty-session check.	<i>disable</i>	Disable strict dirty-session check.			
	Option	Description								
	<i>enable</i>	Enable strict dirty-session check.								
<i>disable</i>	Disable strict dirty-session check.									
strong-crypto	Enable to use strong encryption and only allow strong ciphers and digest for HTTPS/SSH/TLS/SSL functions.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strong crypto for HTTPS/SSH/TLS/SSL.</td></tr><tr><td><i>disable</i></td><td>Disable strong crypto for HTTPS/SSH/TLS/SSL.</td></tr></table>	Option	Description	<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.	<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.			
	Option	Description								
	<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.								
<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.									
switch-controller *	Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from the FortiGate itself.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable switch controller feature.</td></tr><tr><td><i>enable</i></td><td>Enable switch controller feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable switch controller feature.	<i>enable</i>	Enable switch controller feature.			
	Option	Description								
	<i>disable</i>	Disable switch controller feature.								
<i>enable</i>	Enable switch controller feature.									
switch-controller-reserved-network *	Configure reserved network subnet for managed switches. This is available when the switch controller is enabled.	ipv4-classnet-host	Not Specified	10.255.0.1 255.255.0.0						
sys-perf-log-interval	Time in minutes between updates of performance statistics logging. (1 - 15 min, default = 5, 0 = disabled).	integer	Minimum value: 0 Maximum value: 15	5						
syslog-affinity *	Affinity setting for syslog (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0						
tcp-halfclose-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded (1 - 86400 sec (1 day), default = 120).	integer	Minimum value: 1 Maximum value: 86400	120						

Parameter	Description	Type	Size	Default						
tcp-halfopen-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded (1 - 86400 sec (1 day), default = 10).	integer	Minimum value: 1 Maximum value: 86400	10						
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable TCP option.</td></tr><tr><td>disable</td><td>Disable TCP option.</td></tr></table>	Option	Description	enable	Enable TCP option.	disable	Disable TCP option.			
Option	Description									
enable	Enable TCP option.									
disable	Disable TCP option.									
tcp-rst-timer	Length of the TCP CLOSE state in seconds (5 - 300 sec, default = 5).	integer	Minimum value: 5 Maximum value: 300	5						
tcp-timewait-timer	Length of the TCP TIME-WAIT state in seconds (1 - 300 sec, default = 1).	integer	Minimum value: 0 Maximum value: 300	1						
telemetry-controller *	Enable/disable FortiTelemetry controller to manage FortiTelemetry agents.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiTelemetry controller.</td></tr><tr><td>disable</td><td>Disable FortiTelemetry controller.</td></tr></table>	Option	Description	enable	Enable FortiTelemetry controller.	disable	Disable FortiTelemetry controller.			
Option	Description									
enable	Enable FortiTelemetry controller.									
disable	Disable FortiTelemetry controller.									
telemetry-data-port *	FortiTelemetry data channel port (1024 - 49150, default = 35246).	integer	Minimum value: 1024 Maximum value: 49150	35246						
tftp	Enable/disable TFTP.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable TFTP.</td></tr><tr><td>disable</td><td>Disable TFTP.</td></tr></table>	Option	Description	enable	Enable TFTP.	disable	Disable TFTP.			
Option	Description									
enable	Enable TFTP.									
disable	Disable TFTP.									
timezone	Timezone database name. Enter ? to view the list of timezone.	string	Maximum length: 63							
tls-session-cache	Enable/disable TLS session cache.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable TLS session cache.		
	<i>disable</i>	Disable TLS session cache.		
traffic-priority	Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping.	option	-	tos
	Option	Description		
	<i>tos</i>	IP TOS.		
	<i>dscp</i>	DSCP (DiffServ) DS.		
traffic-priority-level	Default system-wide level of priority for traffic prioritization.	option	-	medium
	Option	Description		
	<i>low</i>	Low priority.		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		
two-factor-email-expiry	Email-based two-factor authentication session timeout (30 - 300 seconds (5 minutes), default = 60).	integer	Minimum value: 30 Maximum value: 300	60
two-factor-fac-expiry	FortiAuthenticator token authentication session timeout (10 - 3600 seconds (1 hour), default = 60).	integer	Minimum value: 10 Maximum value: 3600	60
two-factor-ftk-expiry	FortiToken authentication session timeout (60 - 600 sec (10 minutes), default = 60).	integer	Minimum value: 60 Maximum value: 600	60
two-factor-ftm-expiry	FortiToken Mobile session timeout (1 - 168 hours (7 days), default = 72).	integer	Minimum value: 1 Maximum value: 168	72
two-factor-sms-expiry	SMS-based two-factor authentication session timeout (30 - 300 sec, default = 60).	integer	Minimum value: 30 Maximum value: 300	60

Parameter	Description	Type	Size	Default						
udp-idle-timer	UDP connection session timeout. This command can be useful in managing CPU and memory resources (1 - 86400 seconds (1 day), default = 60).	integer	Minimum value: 1 Maximum value: 86400	180						
upgrade-report	Enable/disable the generation of an upgrade report when upgrading the firmware.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable to automatically generate upgrade report when upgrading the firmware.</td></tr><tr><td>disable</td><td>Disable upgrade report generation when upgrading the firmware.</td></tr></table>				Option	Description	enable	Enable to automatically generate upgrade report when upgrading the firmware.	disable	Disable upgrade report generation when upgrading the firmware.
Option	Description									
enable	Enable to automatically generate upgrade report when upgrading the firmware.									
disable	Disable upgrade report generation when upgrading the firmware.									
url-filter-affinity *	URL filter CPU affinity.	string	Maximum length: 79	0						
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 1 **	1						
user-device-store-max-device-mem	Maximum percentage of total system memory allowed to be used for devices in the user device store.	integer	Minimum value: 1 Maximum value: 5	2						
user-device-store-max-devices	Maximum number of devices allowed in user device store.	integer	Minimum value: 84219 Maximum value: 240627 **	168438 **						
user-device-store-max-unified-mem	Maximum unified memory allowed in user device store.	integer	Minimum value: 168438988 Maximum value: 168438988 **	842194944 **						
user-device-store-max-users	Maximum number of users allowed in user device store.	integer	Minimum value: 84219 Maximum value: 240627 **	168438 **						
user-history-password-threshold	Maximum number of previous passwords saved per admin/user (3 - 15, default = 3).	integer	Minimum value: 3 Maximum value: 15	3						

Parameter	Description	Type	Size	Default						
vdom-mode *	Enable/disable support for multiple virtual domains (VDOMs).	option	-	no-vdom						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no-vdom</td><td>Disable multiple VDOMs mode.</td></tr><tr><td>multi-vdom</td><td>Enable multiple VDOMs mode.</td></tr></table>	Option	Description	no-vdom	Disable multiple VDOMs mode.	multi-vdom	Enable multiple VDOMs mode.			
Option	Description									
no-vdom	Disable multiple VDOMs mode.									
multi-vdom	Enable multiple VDOMs mode.									
vip-arp-range	Controls the number of ARPs that the FortiGate sends for a Virtual IP (VIP) address range.	option	-	restricted						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>unlimited</td><td>Send ARPs for all addresses in VIP range.</td></tr><tr><td>restricted</td><td>Send ARPs for the first 8192 addresses in VIP range.</td></tr></table>	Option	Description	unlimited	Send ARPs for all addresses in VIP range.	restricted	Send ARPs for the first 8192 addresses in VIP range.			
Option	Description									
unlimited	Send ARPs for all addresses in VIP range.									
restricted	Send ARPs for the first 8192 addresses in VIP range.									
virtual-switch-vlan *	Enable/disable virtual switch VLAN.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable virtual switch VLAN.</td></tr><tr><td>disable</td><td>Disable virtual switch VLAN.</td></tr></table>	Option	Description	enable	Enable virtual switch VLAN.	disable	Disable virtual switch VLAN.			
Option	Description									
enable	Enable virtual switch VLAN.									
disable	Disable virtual switch VLAN.									
wad-affinity *	Affinity setting for wad (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0						
wad-csvc-cs-count	Number of concurrent WAD-cache-service object-cache processes.	integer	Minimum value: 1 Maximum value: 1							
wad-csvc-db-count	Number of concurrent WAD-cache-service byte-cache processes.	integer	Minimum value: 0 Maximum value: 8 **							
wad-memory-change-granularity	Minimum percentage change in system memory usage detected by the wad daemon prior to adjusting TCP window size for any active connection.	integer	Minimum value: 5 Maximum value: 25	10						
wad-p2s-max-body-size	Maximum size of the body of the local out HTTP request (1 - 32 Mbytes, default = 4).	integer	Minimum value: 1 Maximum value: 32	4						
wad-restart-end-time	WAD workers daily restart end time (hh:mm).	user	Not Specified							

Parameter	Description	Type	Size	Default
wad-restart-mode	WAD worker restart mode (default = none).	option	-	none
	Option	Description		
	<i>none</i>	Disable restart of WAD workers.		
	<i>time</i>	Enable daily restart of WAD workers.		
	<i>memory</i>	Enable restart of WAD workers based on memory usage.		
wad-restart-start-time	WAD workers daily restart time (hh:mm).	user	Not Specified	
wad-source-affinity	Enable/disable dispatching traffic to WAD workers based on source affinity.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable dispatching traffic to WAD workers based on source affinity.		
	<i>enable</i>	Enable dispatching traffic to WAD workers based on source affinity.		
wad-worker-count	Number of explicit proxy WAN optimization daemon (WAD) processes. By default WAN optimization, explicit proxy, and web caching is handled by all of the CPU cores in a FortiGate unit.	integer	Minimum value: 0 0 Maximum value: 8 **	
wifi-ca-certificate	CA certificate that verifies the WiFi certificate.	string	Maximum length: 79	Fortinet_Wifi_CA
wifi-certificate	Certificate to use for WiFi authentication.	string	Maximum length: 35	Fortinet_Wifi
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WiMax 4G.		
	<i>disable</i>	Disable WiMax 4G.		
wireless-controller	Enable/disable the wireless controller feature to use the FortiGate unit to manage FortiAPs.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable wireless controller.		
	<i>disable</i>	Disable wireless controller.		
wireless-controller-port	Port used for the control channel in wireless controller mode (wireless-mode is ac). The data channel port is the control channel port number plus one (1024 - 49150, default = 5246).	integer	Minimum value: 1024 Maximum value: 49150	5246
wireless-mode *	Wireless mode setting.	option	-	ac
	Option	Description		
	<i>ac</i>	Wireless controller with local wireless.		
	<i>client</i>	Wireless client mode.		
	<i>fwfap</i>	Obsolete wireless AP mode.		

* This parameter may not exist in some models.

** Values may differ between models.

config split-port-mode

Parameter	Description	Type	Size	Default																
interface	Split port interface.	string	Maximum length: 15																	
split-mode	The configuration mode for the split port interface.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable split.</td></tr><tr><td><i>4x10G</i></td><td>Split the port into four 10G ports.</td></tr><tr><td><i>4x25G</i></td><td>Split the port into four 25G ports.</td></tr><tr><td><i>4x50G</i></td><td>Split the port into four 50G ports.</td></tr><tr><td><i>8x50G</i></td><td>Split the port into eight 50G ports.</td></tr><tr><td><i>4x100G</i></td><td>Split the port into four 100G ports.</td></tr><tr><td><i>2x200G</i></td><td>Split the port into two 200G ports.</td></tr></table>				Option	Description	<i>disable</i>	Disable split.	<i>4x10G</i>	Split the port into four 10G ports.	<i>4x25G</i>	Split the port into four 25G ports.	<i>4x50G</i>	Split the port into four 50G ports.	<i>8x50G</i>	Split the port into eight 50G ports.	<i>4x100G</i>	Split the port into four 100G ports.	<i>2x200G</i>	Split the port into two 200G ports.
Option	Description																			
<i>disable</i>	Disable split.																			
<i>4x10G</i>	Split the port into four 10G ports.																			
<i>4x25G</i>	Split the port into four 25G ports.																			
<i>4x50G</i>	Split the port into four 50G ports.																			
<i>8x50G</i>	Split the port into eight 50G ports.																			
<i>4x100G</i>	Split the port into four 100G ports.																			
<i>2x200G</i>	Split the port into two 200G ports.																			

config system gre-tunnel

Configure GRE tunnel.

```
config system gre-tunnel
  Description: Configure GRE tunnel.
  edit <name>
    set auto-asic-offload [enable|disable]
    set checksum-reception [disable|enable]
    set checksum-transmission [disable|enable]
    set diffservcode {user}
    set dscp-copying [disable|enable]
    set interface {string}
    set ip-version [4|6]
    set keepalive-failtimes {integer}
    set keepalive-interval {integer}
    set key-inbound {integer}
    set key-outbound {integer}
    set local-gw {ipv4-address-any}
    set local-gw6 {ipv6-address}
    set remote-gw {ipv4-address}
    set remote-gw6 {ipv6-address}
    set sequence-number-reception [disable|enable]
    set sequence-number-transmission [disable|enable]
    set use-sdwan [disable|enable]
  next
end
```

config system gre-tunnel

Parameter	Description	Type	Size	Default
auto-asic-offload *	Enable/disable automatic ASIC offloading.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable automatic ASIC offloading.	
		<i>disable</i>	Disable automatic ASIC offloading.	
checksum-reception *	Enable/disable validating checksums in received GRE packets.	option	-	disable
		Option	Description	
		<i>disable</i>	Do not validate checksums in received GRE packets.	
		<i>enable</i>	Validate checksums in received GRE packets.	

Parameter	Description	Type	Size	Default						
checksum-transmission *	Enable/disable including checksums in transmitted GRE packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not include checksums in transmitted GRE packets.</td></tr><tr><td>enable</td><td>Include checksums in transmitted GRE packets.</td></tr></table>	Option	Description	disable	Do not include checksums in transmitted GRE packets.	enable	Include checksums in transmitted GRE packets.			
Option	Description									
disable	Do not include checksums in transmitted GRE packets.									
enable	Include checksums in transmitted GRE packets.									
diffservcode	DiffServ setting to be applied to GRE tunnel outer IP header.	user	Not Specified							
dscp-copying	Enable/disable DSCP copying.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable DSCP copying.</td></tr><tr><td>enable</td><td>Enable DSCP copying.</td></tr></table>	Option	Description	disable	Disable DSCP copying.	enable	Enable DSCP copying.			
Option	Description									
disable	Disable DSCP copying.									
enable	Enable DSCP copying.									
interface	Interface name.	string	Maximum length: 15							
ip-version	IP version to use for VPN interface.	option	-	4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for gateways.</td></tr><tr><td>6</td><td>Use IPv6 addressing for gateways.</td></tr></table>	Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.			
Option	Description									
4	Use IPv4 addressing for gateways.									
6	Use IPv6 addressing for gateways.									
keepalive-failtimes	Number of consecutive unreturned keepalive messages before a GRE connection is considered down (1 - 255).	integer	Minimum value: 1 Maximum value: 255	10						
keepalive-interval	Keepalive message interval (0 - 32767, 0 = disabled).	integer	Minimum value: 0 Maximum value: 32767	0						
key-inbound *	Require received GRE packets contain this key (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0						
key-outbound *	Include this key in transmitted GRE packets (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0						
local-gw	IP address of the local gateway.	ipv4-address-any	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default
local-gw6	IPv6 address of the local gateway.	ipv6-address	Not Specified	::
name	Tunnel name.	string	Maximum length: 15	
remote-gw	IP address of the remote gateway.	ipv4-address	Not Specified	0.0.0.0
remote-gw6	IPv6 address of the remote gateway.	ipv6-address	Not Specified	::
sequence-number-reception *	Enable/disable validating sequence numbers in received GRE packets.	option	-	disable
	Option		Description	
	<i>disable</i>		Do not validate sequence number in received GRE packets.	
	<i>enable</i>		Validate sequence numbers in received GRE packets.	
sequence-number-transmission *	Enable/disable including of sequence numbers in transmitted GRE packets.	option	-	disable
	Option		Description	
	<i>disable</i>		Include sequence numbers in transmitted GRE packets.	
	<i>enable</i>		Do not include sequence numbers in transmitted GRE packets.	
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable
	Option		Description	
	<i>disable</i>		Disable use of SD-WAN to reach remote gateway.	
	<i>enable</i>		Enable use of SD-WAN to reach remote gateway.	

* This parameter may not exist in some models.

config system ha

Configure HA.

```
config system ha
  Description: Configure HA.
  set arps {integer}
  set arps-interval {integer}
```

```

set authentication [enable|disable]
set auto-virtual-mac-interface <interface-name1>, <interface-name2>, ...
set backup-hbdev <name1>, <name2>, ...
set check-secondary-dev-health [enable|disable]
set cpu-threshold {user}
set encryption [enable|disable]
set evpn-ttl {integer}
set failover-hold-time {integer}
set ftp-proxy-threshold {user}
set gratuitous-arps [enable|disable]
set group-id {integer}
set group-name {string}
set ha-direct [enable|disable]
set ha-eth-type {string}
config ha-mgmt-interfaces
    Description: Reserve interfaces to manage individual cluster units.
    edit <id>
        set dst {ipv4-classnet}
        set dst6 {ipv6-prefix}
        set gateway {ipv4-address}
        set gateway6 {ipv6-address}
        set interface {string}
    next
end
set ha-mgmt-status [enable|disable]
set ha-uptime-diff-margin {integer}
set hb-interval {integer}
set hb-interval-in-milliseconds [100ms|10ms]
set hb-lost-threshold {integer}
set hbdev {user}
set hc-eth-type {string}
set hello-holddown {integer}
set http-proxy-threshold {user}
set imap-proxy-threshold {user}
set ipsec-phase2-proposal {option1}, {option2}, ...
set key {password}
set l2ep-eth-type {string}
set link-failed-signal [enable|disable]
set load-balance-all [enable|disable]
set logical-sn [enable|disable]
set memory-based-failover [enable|disable]
set memory-compatible-mode [enable|disable]
set memory-failover-flip-timeout {integer}
set memory-failover-monitor-period {integer}
set memory-failover-sample-rate {integer}
set memory-failover-threshold {integer}
set memory-threshold {user}
set mode [standalone|a-a|...]
set monitor {user}
set multicast-ttl {integer}
set nntp-proxy-threshold {user}
set override [enable|disable]

```



```

set override-wait-time {integer}
set password {password}
set pingserver-failover-threshold {integer}
set pingserver-flip-timeout {integer}
set pingserver-monitor-interface {user}
set pingserver-secondary-force-reset [enable|disable]
set pop3-proxy-threshold {user}
set priority {integer}
set route-hold {integer}
set route-ttl {integer}
set route-wait {integer}
set schedule [none|leastconnection|...]
set session-pickup [enable|disable]
set session-pickup-connectionless [enable|disable]
set session-pickup-delay [enable|disable]
set session-pickup-expectation [enable|disable]
set session-pickup-nat [enable|disable]
set session-sync-dev {user}
set smtp-proxy-threshold {user}
set ssd-failover [enable|disable]
set standalone-config-sync [enable|disable]
set standalone-mgmt-vdom [enable|disable]
set sync-config [enable|disable]
set sync-packet-balance [enable|disable]
set unicast-gateway {ipv4-address}
set unicast-hb [enable|disable]
set unicast-hb-netmask {ipv4-netmask}
set unicast-hb-peerip {ipv4-address}
config unicast-peers
    Description: Number of unicast peers.
    edit <id>
        set peer-ip {ipv4-address}
    next
end
set unicast-status [enable|disable]
set uninterruptible-primary-wait {integer}
set upgrade-mode [simultaneous|uninterruptible|...]
config vcluster
    Description: Virtual cluster table.
    edit <vcluster-id>
        set monitor {user}
        set override [enable|disable]
        set override-wait-time {integer}
        set pingserver-failover-threshold {integer}
        set pingserver-flip-timeout {integer}
        set pingserver-monitor-interface {user}
        set pingserver-secondary-force-reset [enable|disable]
        set priority {integer}
        set vdom <name1>, <name2>, ...
    next
end
set vcluster-status [enable|disable]

```

```

    set weight {user}
end

```

config system ha

Parameter	Description	Type	Size	Default						
arps	Number of gratuitous ARPs (1 - 60). Lower to reduce traffic. Higher to reduce failover time.	integer	Minimum value: 1 Maximum value: 60	5						
arps-interval	Time between gratuitous ARPs (1 - 20 sec). Lower to reduce failover time. Higher to reduce traffic.	integer	Minimum value: 1 Maximum value: 20	8						
authentication	Enable/disable heartbeat message authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable heartbeat message authentication.</td></tr><tr><td><i>disable</i></td><td>Disable heartbeat message authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable heartbeat message authentication.	<i>disable</i>	Disable heartbeat message authentication.			
Option	Description									
<i>enable</i>	Enable heartbeat message authentication.									
<i>disable</i>	Disable heartbeat message authentication.									
auto-virtual-mac-interface <interface-name>	The physical interface that will be assigned an auto-generated virtual MAC address. Interface name.	string	Maximum length: 15							
backup-hbdev <name>	Backup heartbeat interfaces. Must be the same for all members. Interface name.	string	Maximum length: 79							
check-secondary-dev-health	Enable/disable secondary dev health check for session load-balance in HA A-A mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
cpu-threshold	Dynamic weighted load balancing CPU usage weight and high and low thresholds.	user	Not Specified							
encryption	Enable/disable heartbeat message encryption.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable heartbeat message encryption.		
	<i>disable</i>	Disable heartbeat message encryption.		
evpn-ttl	HA EVPN FDB TTL on primary box (5 - 3600 sec).	integer	Minimum value: 5 Maximum value: 3600	60
failover-hold-time	Time to wait before failover (0 - 300 sec, default = 0), to avoid flip.	integer	Minimum value: 0 Maximum value: 300	0
ftp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of FTP proxy sessions.	user	Not Specified	
gratuitous-arps	Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable gratuitous ARPs.		
	<i>disable</i>	Disable gratuitous ARPs.		
group-id	HA group ID (0 - 1023; or 0 - 7 when there are more than 2 vclusters). Must be the same for all members.	integer	Minimum value: 0 Maximum value: 1023	0
group-name	Cluster group name. Must be the same for all members.	string	Maximum length: 32	
ha-direct	Enable/disable using ha-mgmt interface for syslog, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable using ha-mgmt interface for syslog, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.		
	<i>disable</i>	Disable using ha-mgmt interface for syslog, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.		

Parameter	Description	Type	Size	Default						
ha-eth-type	HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8890						
ha-mgmt-status	Enable to reserve interfaces to manage individual cluster units.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ha-uptime-diff-margin	Normally you would only reduce this value for failover testing.	integer	Minimum value: 1 Maximum value: 65535	300						
hb-interval	Time between sending heartbeat packets (1 - 20). Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20	2						
hb-interval-in-milliseconds	Units of heartbeat interval time between sending heartbeat packets. Default is 100ms.	option	-	100ms						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>100ms</i></td><td>Each heartbeat interval is 100ms.</td></tr><tr><td><i>10ms</i></td><td>Each heartbeat interval is 10ms.</td></tr></table>	Option	Description	<i>100ms</i>	Each heartbeat interval is 100ms.	<i>10ms</i>	Each heartbeat interval is 10ms.			
Option	Description									
<i>100ms</i>	Each heartbeat interval is 100ms.									
<i>10ms</i>	Each heartbeat interval is 10ms.									
hb-lost-threshold	Number of lost heartbeats to signal a failure (1 - 60). Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60	6 **						
hbdev	Heartbeat interfaces. Must be the same for all members. Enter <interface> <priority> pairs to specify the priority of each heartbeat interface. Higher priority takes precedence.	user	Not Specified							
hc-eth-type	Transparent mode HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8891						
hello-holddown	Time to wait before changing from hello to work state (5 - 300 sec).	integer	Minimum value: 5 Maximum value: 300	20						

Parameter	Description	Type	Size	Default																																	
http-proxy-threshold	Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.	user	Not Specified																																		
imap-proxy-threshold	Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.	user	Not Specified																																		
ipsec-phase2-proposal	IPsec phase2 proposal.	option	-																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aes128-sha1</i></td><td>aes128-sha1</td></tr><tr><td><i>aes128-sha256</i></td><td>aes128-sha256</td></tr><tr><td><i>aes128-sha384</i></td><td>aes128-sha384</td></tr><tr><td><i>aes128-sha512</i></td><td>aes128-sha512</td></tr><tr><td><i>aes192-sha1</i></td><td>aes192-sha1</td></tr><tr><td><i>aes192-sha256</i></td><td>aes192-sha256</td></tr><tr><td><i>aes192-sha384</i></td><td>aes192-sha384</td></tr><tr><td><i>aes192-sha512</i></td><td>aes192-sha512</td></tr><tr><td><i>aes256-sha1</i></td><td>aes256-sha1</td></tr><tr><td><i>aes256-sha256</i></td><td>aes256-sha256</td></tr><tr><td><i>aes256-sha384</i></td><td>aes256-sha384</td></tr><tr><td><i>aes256-sha512</i></td><td>aes256-sha512</td></tr><tr><td><i>aes128gcm</i></td><td>aes128gcm</td></tr><tr><td><i>aes256gcm</i></td><td>aes256gcm</td></tr><tr><td><i>chacha20poly1305</i></td><td>chacha20poly1305</td></tr></table>		Option	Description	<i>aes128-sha1</i>	aes128-sha1	<i>aes128-sha256</i>	aes128-sha256	<i>aes128-sha384</i>	aes128-sha384	<i>aes128-sha512</i>	aes128-sha512	<i>aes192-sha1</i>	aes192-sha1	<i>aes192-sha256</i>	aes192-sha256	<i>aes192-sha384</i>	aes192-sha384	<i>aes192-sha512</i>	aes192-sha512	<i>aes256-sha1</i>	aes256-sha1	<i>aes256-sha256</i>	aes256-sha256	<i>aes256-sha384</i>	aes256-sha384	<i>aes256-sha512</i>	aes256-sha512	<i>aes128gcm</i>	aes128gcm	<i>aes256gcm</i>	aes256gcm	<i>chacha20poly1305</i>	chacha20poly1305			
	Option	Description																																			
	<i>aes128-sha1</i>	aes128-sha1																																			
	<i>aes128-sha256</i>	aes128-sha256																																			
	<i>aes128-sha384</i>	aes128-sha384																																			
	<i>aes128-sha512</i>	aes128-sha512																																			
	<i>aes192-sha1</i>	aes192-sha1																																			
	<i>aes192-sha256</i>	aes192-sha256																																			
	<i>aes192-sha384</i>	aes192-sha384																																			
	<i>aes192-sha512</i>	aes192-sha512																																			
	<i>aes256-sha1</i>	aes256-sha1																																			
	<i>aes256-sha256</i>	aes256-sha256																																			
	<i>aes256-sha384</i>	aes256-sha384																																			
	<i>aes256-sha512</i>	aes256-sha512																																			
	<i>aes128gcm</i>	aes128gcm																																			
	<i>aes256gcm</i>	aes256gcm																																			
<i>chacha20poly1305</i>	chacha20poly1305																																				
key	Key.	password	Not Specified																																		
l2ep-eth-type	Telnet session HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8893																																	
link-failed-signal	Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.	option	-	disable																																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
load-balance-all	Enable to load balance TCP sessions. Disable to load balance proxy sessions only.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable load balance.		
	<i>disable</i>	Disable load balance.		
logical-sn *	Enable/disable usage of the logical serial number.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable usage of the logical serial number.		
	<i>disable</i>	Disable usage of the logical serial number.		
memory-based-failover	Enable/disable memory based failover.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
memory-compatible-mode	Enable/disable memory compatible mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
memory-failover-flip-timeout	Time to wait between subsequent memory based failovers in minutes (6 - 2147483647, default = 6).	integer	Minimum value: 6 Maximum value: 2147483647	6

Parameter	Description	Type	Size	Default								
memory-failover-monitor-period	Duration of high memory usage before memory based failover is triggered in seconds (1 - 300, default = 60).	integer	Minimum value: 1 Maximum value: 300	60								
memory-failover-sample-rate	Rate at which memory usage is sampled in order to measure memory usage in seconds (1 - 60, default = 1).	integer	Minimum value: 1 Maximum value: 60	1								
memory-failover-threshold	Memory usage threshold to trigger memory based failover (0 means using conserve mode threshold in system.global).	integer	Minimum value: 0 Maximum value: 95	0								
memory-threshold	Dynamic weighted load balancing memory usage weight and high and low thresholds.	user	Not Specified									
mode	HA mode. Must be the same for all members. FGSP requires standalone.	option	-	standalone								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standalone</i></td><td>Standalone mode.</td></tr><tr><td><i>a-a</i></td><td>Active-active mode.</td></tr><tr><td><i>a-p</i></td><td>Active-passive mode.</td></tr></table>				Option	Description	<i>standalone</i>	Standalone mode.	<i>a-a</i>	Active-active mode.	<i>a-p</i>	Active-passive mode.
Option	Description											
<i>standalone</i>	Standalone mode.											
<i>a-a</i>	Active-active mode.											
<i>a-p</i>	Active-passive mode.											
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified									
multicast-ttl	HA multicast TTL on primary (5 - 3600 sec).	integer	Minimum value: 5 Maximum value: 3600	600								
nntp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of NNTP proxy sessions.	user	Not Specified									
override	Enable and increase the priority of the unit that should always be primary (master).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

Parameter	Description	Type	Size	Default
override-wait-time	Delay negotiating if override is enabled (0 - 3600 sec). Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0
password	Cluster password. Must be the same for all members.	password	Not Specified	
pingserver-failover-threshold	Remote IP monitoring failover threshold (0 - 50).	integer	Minimum value: 0 Maximum value: 50	0
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647	60
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified	
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable
	Option	Description		
	enable	Enable force reset of secondary member after PING server failure.		
	disable	Disable force reset of secondary member after PING server failure.		
pop3-proxy-threshold	Dynamic weighted load balancing weight and high and low number of POP3 proxy sessions.	user	Not Specified	
priority	Increase the priority to select the primary unit (0 - 255).	integer	Minimum value: 0 Maximum value: 255	128
route-hold	Time to wait between routing table updates to the cluster (0 - 3600 sec).	integer	Minimum value: 0 Maximum value: 3600	10
route-ttl	TTL for primary unit routes (5 - 3600 sec). Increase to maintain active routes during failover.	integer	Minimum value: 5 Maximum value: 3600	10

Parameter	Description	Type	Size	Default																
route-wait	Time to wait before sending new routes to the cluster (0 - 3600 sec).	integer	Minimum value: 0 Maximum value: 3600	0																
schedule	Type of A-A load balancing. Use none if you have external load balancers.	option	-	round-robin																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>leastconnection</i></td><td>Least connection.</td></tr><tr><td><i>round-robin</i></td><td>Round robin.</td></tr><tr><td><i>weight-round-robin</i></td><td>Weight round robin.</td></tr><tr><td><i>random</i></td><td>Random.</td></tr><tr><td><i>ip</i></td><td>IP.</td></tr><tr><td><i>ipport</i></td><td>IP port.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>leastconnection</i>	Least connection.	<i>round-robin</i>	Round robin.	<i>weight-round-robin</i>	Weight round robin.	<i>random</i>	Random.	<i>ip</i>	IP.	<i>ipport</i>	IP port.			
Option	Description																			
<i>none</i>	None.																			
<i>leastconnection</i>	Least connection.																			
<i>round-robin</i>	Round robin.																			
<i>weight-round-robin</i>	Weight round robin.																			
<i>random</i>	Random.																			
<i>ip</i>	IP.																			
<i>ipport</i>	IP port.																			
session-pickup	Enable/disable session pickup. Enabling it can reduce session down time when fail over happens.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable session pickup.</td></tr><tr><td><i>disable</i></td><td>Disable session pickup.</td></tr></table>	Option	Description	<i>enable</i>	Enable session pickup.	<i>disable</i>	Disable session pickup.													
Option	Description																			
<i>enable</i>	Enable session pickup.																			
<i>disable</i>	Disable session pickup.																			
session-pickup-connectionless	Enable/disable UDP and ICMP session sync.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.													
Option	Description																			
<i>enable</i>	Enable setting.																			
<i>disable</i>	Disable setting.																			
session-pickup-delay	Enable to sync sessions longer than 30 sec. Only longer lived sessions need to be synced.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.													
Option	Description																			
<i>enable</i>	Enable setting.																			
<i>disable</i>	Disable setting.																			

Parameter	Description	Type	Size	Default						
session-pickup-expectation	Enable/disable session helper expectation session sync for FGSP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
session-pickup-nat	Enable/disable NAT session sync for FGSP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified							
smtp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of SMTP proxy sessions.	user	Not Specified							
ssd-failover *	Enable/disable automatic HA failover on SSD disk failure.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
standalone-config-sync	Enable/disable FGSP configuration synchronization.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
standalone-mgmt-vdom	Enable/disable standalone management VDOM.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
sync-config	Enable/disable configuration synchronization.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable configuration synchronization.		
	<i>disable</i>	Disable configuration synchronization.		
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HA packet distribution to multiple CPUs.		
	<i>disable</i>	Disable HA packet distribution to multiple CPUs.		
unicast-gateway *	Default route gateway for unicast interface.	ipv4-address	Not Specified	0.0.0.0
unicast-hb *	Enable/disable unicast heartbeat.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
unicast-hb-netmask *	Unicast heartbeat netmask.	ipv4-netmask	Not Specified	0.0.0.0
unicast-hb-peerip *	Unicast heartbeat peer IP.	ipv4-address	Not Specified	0.0.0.0
unicast-status *	Enable/disable unicast connection.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
uninterruptible-primary-wait	Number of minutes the primary HA unit waits before the secondary HA unit is considered upgraded and the system is started before starting its own upgrade (15 - 300, default = 30).	integer	Minimum value: 15 Maximum value: 300	30
upgrade-mode	The mode to upgrade a cluster.	option	-	uninterruptible

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>simultaneous</i>	Upgrade all HA members at the same time.		
	<i>uninterruptible</i>	Upgrade HA cluster without blocking network traffic.		
	<i>local-only</i>	Upgrade local member only.		
	<i>secondary-only</i>	Upgrade secondary member only.		
vcluster-status	Enable/disable virtual cluster for virtual clustering.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
weight	Weight-round-robin weight for each cluster unit. Syntax <priority> <weight>.	user	Not Specified	0 40

* This parameter may not exist in some models.

** Values may differ between models.

config ha-mgmt-interfaces

Parameter	Description	Type	Size	Default
dst	Default route destination for reserved HA management interface.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
dst6	Default IPv6 destination for reserved HA management interface.	ipv6-prefix	Not Specified	::/0
gateway	Default route gateway for reserved HA management interface.	ipv4-address	Not Specified	0.0.0.0
gateway6	Default IPv6 gateway for reserved HA management interface.	ipv6-address	Not Specified	::
id	Table ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
interface	Interface to reserve for HA management.	string	Maximum length: 15	

config unicast-peers

Parameter	Description	Type	Size	Default
id	Table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
peer-ip	Unicast peer IP.	ipv4-address	Not Specified	0.0.0.0

config vcluster

Parameter	Description	Type	Size	Default
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified	
override	Enable and increase the priority of the unit that should always be primary (master).	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
override-wait-time	Delay negotiating if override is enabled (0 - 3600 sec). Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0
pingserver-failover-threshold	Remote IP monitoring failover threshold (0 - 50).	integer	Minimum value: 0 Maximum value: 50	0
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647	60
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified	
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable force reset of secondary member after PING server failure.		
	<i>disable</i>	Disable force reset of secondary member after PING server failure.		
priority	Increase the priority to select the primary unit (0 - 255).	integer	Minimum value: 0 Maximum value: 255	128
vcluster-id	ID.	integer	Minimum value: 1 Maximum value: 30	1
vdom <name>	Virtual domain(s) in the virtual cluster. Virtual domain name.	string	Maximum length: 79	

config system ha-monitor

Configure HA monitor.

```
config system ha-monitor
  Description: Configure HA monitor.
  set monitor-vlan [enable|disable]
  set vlan-hb-interval {integer}
  set vlan-hb-lost-threshold {integer}
end
```

config system ha-monitor

Parameter	Description	Type	Size	Default						
monitor-vlan	Enable/disable monitor VLAN interfaces.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable monitor VLAN interfaces.</td></tr><tr><td><i>disable</i></td><td>Disable monitor VLAN interfaces.</td></tr></table>				Option	Description	<i>enable</i>	Enable monitor VLAN interfaces.	<i>disable</i>	Disable monitor VLAN interfaces.
	Option	Description								
	<i>enable</i>	Enable monitor VLAN interfaces.								
<i>disable</i>	Disable monitor VLAN interfaces.									
vlan-hb-interval	Configure heartbeat interval (seconds).	integer	Minimum value: 1 Maximum value: 30	5						

Parameter	Description	Type	Size	Default
vlan-hb-lost-threshold	VLAN lost heartbeat threshold (1 - 60).	integer	Minimum value: 1 Maximum value: 60	3

config system health-check-fortiguard

SD-WAN status checking or health checking. Identify a server predefined by FortiGuard and determine how SD-WAN verifies that FGT can communicate with it.

```
config system health-check-fortiguard
    Description: SD-WAN status checking or health checking. Identify a server predefined by
    FortiGuard and determine how SD-WAN verifies that FGT can communicate with it.
    edit <name>
        set obsolete {integer}
        set protocol [ping|tcp-echo|...]
        set server {string}
    next
end
```

config system health-check-fortiguard

Parameter	Description	Type	Size	Default														
name	Status check or predefined health-check targets name.	string	Maximum length: 35															
obsolete	Indicates whether Health Check service can be used. Read-only.	integer	Minimum value: 0 Maximum value: 255	0														
protocol	Protocol name.	option	-	ping														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>Use PING to test the link with the server.</td></tr><tr><td>tcp-echo</td><td>Use TCP echo to test the link with the server.</td></tr><tr><td>udp-echo</td><td>Use UDP echo to test the link with the server.</td></tr><tr><td>http</td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td>https</td><td>Use HTTPS-GET to test the link with the server.</td></tr><tr><td>twamp</td><td>Use TWAMP to test the link with the server.</td></tr></table>	Option	Description	ping	Use PING to test the link with the server.	tcp-echo	Use TCP echo to test the link with the server.	udp-echo	Use UDP echo to test the link with the server.	http	Use HTTP-GET to test the link with the server.	https	Use HTTPS-GET to test the link with the server.	twamp	Use TWAMP to test the link with the server.			
Option	Description																	
ping	Use PING to test the link with the server.																	
tcp-echo	Use TCP echo to test the link with the server.																	
udp-echo	Use UDP echo to test the link with the server.																	
http	Use HTTP-GET to test the link with the server.																	
https	Use HTTPS-GET to test the link with the server.																	
twamp	Use TWAMP to test the link with the server.																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dns</i>	Use DNS query to test the link with the server.		
	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.		
	<i>ftp</i>	Use FTP to test the link with the server.		
server	Status check or predefined health-check domain name.	string	Maximum length: 127	

config system icond



This command is available for model(s): FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure Industrial Connectivity.

```
config system icond
  Description: Configure Industrial Connectivity.
  set iec101-keepalive [disable|enable]
  set iec101-laddr-local {integer}
  set iec101-laddr-remote {integer}
  set iec101-laddr-size {integer}
  set iec101-mode [balanced|unbalanced]
  set iec101-t0 {integer}
  set iec101-trp {integer}
```



```

set iec101-use-ack-char [disable|enable]
set iec104-k {integer}
set iec104-t1 {integer}
set iec104-t2 {integer}
set iec104-t3 {integer}
set iec104-w {integer}
set modbus-serial-addr {integer}
set modbus-serial-mode [RTU|ASCII]
set modbus-serial-timeout-resp {integer}
set modbus-tcp-unit-id {integer}
set port {integer}
set status [disable|enable]
set tty-baudrate [200|300|...]
set tty-databits {integer}
set tty-device {string}
set tty-flowcontrol [none|xon-xoff|...]
set tty-parity [none|odd|...]
set tty-stopbits {integer}
set type [iec101-104|modbus-serial-tcp|...]
end

```

config system icond

Parameter	Description	Type	Size	Default						
iec101-keepalive	Send periodic test frame for probing link status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable the selected function.</td></tr><tr><td><i>enable</i></td><td>Enable the selected function.</td></tr></table>	Option	Description	<i>disable</i>	Disable the selected function.	<i>enable</i>	Enable the selected function.			
Option	Description									
<i>disable</i>	Disable the selected function.									
<i>enable</i>	Enable the selected function.									
iec101-laddr-local	Link address of local.	integer	Minimum value: 1 Maximum value: 65534	1						
iec101-laddr-remote	Link address of remote.	integer	Minimum value: 1 Maximum value: 65535	2						
iec101-laddr-size	Link address size.	integer	Minimum value: 0 Maximum value: 2	1						

Parameter	Description	Type	Size	Default
iec101-mode	Link layer transmission procedure.	option	-	balanced
	Option	Description		
	<i>balanced</i>	Set IEC101 transmission mode to balanced.		
	<i>unbalanced</i>	Set IEC101 transmission mode to unbalanced.		
iec101-t0	Time out for repetition of frames in milliseconds (1 - 30000, default = 500).	integer	Minimum value: 1 Maximum value: 30000	500
iec101-trp	Time interval during which repetitions are permitted in milliseconds (1 - 300000, default = 2500).	integer	Minimum value: 1 Maximum value: 300000	2500
iec101-use-ack-char	Use single character for ACK.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable the selected function.		
	<i>enable</i>	Enable the selected function.		
iec104-k	Maximum number of outstanding I formate APDUs (1 - 32767, default = 12).	integer	Minimum value: 1 Maximum value: 32767	12
iec104-t1	Time-out of send or test APDUs in seconds (1 - 255, default = 15).	integer	Minimum value: 1 Maximum value: 255	15
iec104-t2	Time-out for acknowledges in case no data messages in seconds (1 - 255, default = 10).	integer	Minimum value: 1 Maximum value: 255	10
iec104-t3	Time-out for sending test frames in case of a long idle state in seconds (1 - 172800, default = 20).	integer	Minimum value: 1 Maximum value: 172800	20

Parameter	Description	Type	Size	Default
iec104-w	Maximum number of latest acknowledge APDUs (1 - 32767, default = 8).	integer	Minimum value: 1 Maximum value: 32767	8
modbus-serial-addr	Serial remote station address.	integer	Minimum value: 1 Maximum value: 247	1
modbus-serial-mode	Serial transmission mode.	option	-	RTU
	Option	Description		
	RTU	Set Modbus transmission mode to RTU.		
	ASCII	Set Modbus transmission mode to ASCII.		
modbus-serial-timeout-resp	Time out for serial remote station response in milliseconds (10 - 30000, default = 500).	integer	Minimum value: 10 Maximum value: 30000	500
modbus-tcp-unit-id	TCP MBAP unit identifier.	integer	Minimum value: 0 Maximum value: 255	255
port	Listening socket port.	integer	Minimum value: 1 Maximum value: 65535	0
status	Enable/disable this connection.	option	-	disable
	Option	Description		
	disable	Disable the selected function.		
	enable	Enable the selected function.		
tty-baudrate	TTY baudrate.	option	-	9600
	Option	Description		
	200	Set TTY baudrate to 200.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>300</td><td>Set TTY baudrate to 300.</td></tr><tr><td>600</td><td>Set TTY baudrate to 600.</td></tr><tr><td>1200</td><td>Set TTY baudrate to 1200.</td></tr><tr><td>2400</td><td>Set TTY baudrate to 2400.</td></tr><tr><td>4800</td><td>Set TTY baudrate to 4800.</td></tr><tr><td>9600</td><td>Set TTY baudrate to 9600.</td></tr><tr><td>19200</td><td>Set TTY baudrate to 19200.</td></tr><tr><td>38400</td><td>Set TTY baudrate to 38400.</td></tr><tr><td>115200</td><td>Set TTY baudrate to 115200.</td></tr></table>	Option	Description	300	Set TTY baudrate to 300.	600	Set TTY baudrate to 600.	1200	Set TTY baudrate to 1200.	2400	Set TTY baudrate to 2400.	4800	Set TTY baudrate to 4800.	9600	Set TTY baudrate to 9600.	19200	Set TTY baudrate to 19200.	38400	Set TTY baudrate to 38400.	115200	Set TTY baudrate to 115200.			
	Option	Description																						
	300	Set TTY baudrate to 300.																						
	600	Set TTY baudrate to 600.																						
	1200	Set TTY baudrate to 1200.																						
	2400	Set TTY baudrate to 2400.																						
	4800	Set TTY baudrate to 4800.																						
	9600	Set TTY baudrate to 9600.																						
	19200	Set TTY baudrate to 19200.																						
	38400	Set TTY baudrate to 38400.																						
115200	Set TTY baudrate to 115200.																							
tty-databits	TTY databits.	integer	Minimum value: 5 Maximum value: 8	8																				
tty-device	TTY device.	string	Maximum length: 35	serial0																				
tty-flowcontrol	TTY flowcontrol.	option	-	none																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Set TTY flow control to none.</td></tr><tr><td>xon-xoff</td><td>Set TTY flow control to xon/xoff.</td></tr><tr><td>hw</td><td>Set TTY flow control to hardware.</td></tr></table>	Option	Description	none	Set TTY flow control to none.	xon-xoff	Set TTY flow control to xon/xoff.	hw	Set TTY flow control to hardware.															
	Option	Description																						
	none	Set TTY flow control to none.																						
	xon-xoff	Set TTY flow control to xon/xoff.																						
hw	Set TTY flow control to hardware.																							
tty-parity	TTY parity.	option	-	even																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Set TTY parity to none.</td></tr><tr><td>odd</td><td>Set TTY parity to odd.</td></tr><tr><td>even</td><td>Set TTY parity to even.</td></tr></table>	Option	Description	none	Set TTY parity to none.	odd	Set TTY parity to odd.	even	Set TTY parity to even.															
	Option	Description																						
	none	Set TTY parity to none.																						
	odd	Set TTY parity to odd.																						
even	Set TTY parity to even.																							
tty-stopbits	TTY stopbits.	integer	Minimum value: 1 Maximum value: 2	1																				
type	Connection type.	option	-	iec101-104																				

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>iec101-104</i>	Convert between IEC60870-5-101 and IEC60870-5-104.		
	<i>modbus-serial-tcp</i>	Convert between Modbus Serial and Modbus TCP.		
	<i>raw</i>	Re-direct traffic from TTY to socket without conversion.		

config system ike

Configure IKE global attributes.

```

config system ike
  Description: Configure IKE global attributes.
  config dh-group-1
    Description: Diffie-Hellman group 1 (MODP-768).
    set keypair-cache [global|custom]
    set keypair-count {integer}
    set mode [software|hardware|...]
  end
  config dh-group-14
    Description: Diffie-Hellman group 14 (MODP-2048).
    set keypair-cache [global|custom]
    set keypair-count {integer}
    set mode [software|hardware|...]
  end
  config dh-group-15
    Description: Diffie-Hellman group 15 (MODP-3072).
    set keypair-cache [global|custom]
    set keypair-count {integer}
    set mode [software|hardware|...]
  end
  config dh-group-16
    Description: Diffie-Hellman group 16 (MODP-4096).
    set keypair-cache [global|custom]
    set keypair-count {integer}
    set mode [software|hardware|...]
  end
  config dh-group-17
    Description: Diffie-Hellman group 17 (MODP-6144).
    set keypair-cache [global|custom]
    set keypair-count {integer}
    set mode [software|hardware|...]
  end
  config dh-group-18
    Description: Diffie-Hellman group 18 (MODP-8192).
    set keypair-cache [global|custom]
    set keypair-count {integer}

```

```

        set mode [software|hardware|...]
    end
    config dh-group-19
        Description: Diffie-Hellman group 19 (EC-P256).
        set keypair-cache [global|custom]
        set keypair-count {integer}
        set mode [software|hardware|...]
    end
    config dh-group-2
        Description: Diffie-Hellman group 2 (MODP-1024).
        set keypair-cache [global|custom]
        set keypair-count {integer}
        set mode [software|hardware|...]
    end
    config dh-group-20
        Description: Diffie-Hellman group 20 (EC-P384).
        set keypair-cache [global|custom]
        set keypair-count {integer}
        set mode [software|hardware|...]
    end
    config dh-group-21
        Description: Diffie-Hellman group 21 (EC-P521).
        set keypair-cache [global|custom]
        set keypair-count {integer}
        set mode [software|hardware|...]
    end
    config dh-group-27
        Description: Diffie-Hellman group 27 (EC-P224BP).
        set keypair-cache [global|custom]
        set keypair-count {integer}
        set mode [software|hardware|...]
    end
    config dh-group-28
        Description: Diffie-Hellman group 28 (EC-P256BP).
        set keypair-cache [global|custom]
        set keypair-count {integer}
        set mode [software|hardware|...]
    end
    config dh-group-29
        Description: Diffie-Hellman group 29 (EC-P384BP).
        set keypair-cache [global|custom]
        set keypair-count {integer}
        set mode [software|hardware|...]
    end
    config dh-group-30
        Description: Diffie-Hellman group 30 (EC-P512BP).
        set keypair-cache [global|custom]
        set keypair-count {integer}
        set mode [software|hardware|...]
    end
    config dh-group-31
        Description: Diffie-Hellman group 31 (EC-X25519).

```

```

    set keypair-cache [global|custom]
    set keypair-count {integer}
    set mode [software|hardware|...]
end
config dh-group-32
    Description: Diffie-Hellman group 32 (EC-X448).
    set keypair-cache [global|custom]
    set keypair-count {integer}
    set mode [software|hardware|...]
end
config dh-group-5
    Description: Diffie-Hellman group 5 (MODP-1536).
    set keypair-cache [global|custom]
    set keypair-count {integer}
    set mode [software|hardware|...]
end
set dh-keypair-cache [enable|disable]
set dh-keypair-count {integer}
set dh-keypair-throttle [enable|disable]
set dh-mode [software|hardware]
set dh-multiprocess [enable|disable]
set dh-worker-count {integer}
set embryonic-limit {integer}
end

```

config system ike

Parameter	Description	Type	Size	Default						
dh-keypair-cache	Enable/disable Diffie-Hellman key pair cache.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Diffie-Hellman key pair cache.</td></tr><tr><td><i>disable</i></td><td>Disable Diffie-Hellman key pair cache.</td></tr></table>	Option	Description	<i>enable</i>	Enable Diffie-Hellman key pair cache.	<i>disable</i>	Disable Diffie-Hellman key pair cache.			
Option	Description									
<i>enable</i>	Enable Diffie-Hellman key pair cache.									
<i>disable</i>	Disable Diffie-Hellman key pair cache.									
dh-keypair-count	Number of key pairs to pre-generate for each Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	100 **						
dh-keypair-throttle	Enable/disable Diffie-Hellman key pair cache CPU throttling.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Diffie-Hellman key pair cache CPU throttling.</td></tr><tr><td><i>disable</i></td><td>Disable Diffie-Hellman key pair cache CPU throttling.</td></tr></table>	Option	Description	<i>enable</i>	Enable Diffie-Hellman key pair cache CPU throttling.	<i>disable</i>	Disable Diffie-Hellman key pair cache CPU throttling.			
Option	Description									
<i>enable</i>	Enable Diffie-Hellman key pair cache CPU throttling.									
<i>disable</i>	Disable Diffie-Hellman key pair cache CPU throttling.									

Parameter	Description	Type	Size	Default
dh-mode	Use software (CPU) or hardware (CPX) to perform Diffie-Hellman calculations.	option	-	hardware **
	Option	Description		
	software	Prefer CPU to perform Diffie-Hellman calculations.		
	hardware	Prefer CPX to perform Diffie-Hellman calculations.		
dh-multiprocess	Enable/disable multiprocess Diffie-Hellman daemon for IKE.	option	-	enable
	Option	Description		
	enable	Enable multiprocess Diffie-Hellman for IKE.		
	disable	Disable multiprocess Diffie-Hellman for IKE.		
dh-worker-count	Number of Diffie-Hellman workers to start.	integer	Minimum value: 1 Maximum value: 8 **	0
embryonic-limit	Maximum number of IPsec tunnels to negotiate simultaneously.	integer	Minimum value: 50 Maximum value: 20000	5000 **

** Values may differ between models.

config dh-group-1

Parameter	Description	Type	Size	Default						
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Use global Diffie-Hellman key pair cache setting.</td></tr><tr><td><i>custom</i></td><td>Use custom Diffie-Hellman key pair cache setting.</td></tr></table>	Option	Description	<i>global</i>	Use global Diffie-Hellman key pair cache setting.	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.			
Option	Description									
<i>global</i>	Use global Diffie-Hellman key pair cache setting.									
<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.									
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0						

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option Description			
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-14

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option Description			
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option Description			
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-15

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-16

Parameter	Description	Type	Size	Default								
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>global</td><td>Use global Diffie-Hellman key pair cache setting.</td></tr><tr><td>custom</td><td>Use custom Diffie-Hellman key pair cache setting.</td></tr></table>				Option	Description	global	Use global Diffie-Hellman key pair cache setting.	custom	Use custom Diffie-Hellman key pair cache setting.		
Option	Description											
global	Use global Diffie-Hellman key pair cache setting.											
custom	Use custom Diffie-Hellman key pair cache setting.											
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0								
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>software</td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr><tr><td>hardware</td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr><tr><td>global</td><td>Use global dh-mode setting.</td></tr></table>				Option	Description	software	Prefer CPU to perform Diffie-Hellman calculations.	hardware	Prefer CPX to perform Diffie-Hellman calculations.	global	Use global dh-mode setting.
Option	Description											
software	Prefer CPU to perform Diffie-Hellman calculations.											
hardware	Prefer CPX to perform Diffie-Hellman calculations.											
global	Use global dh-mode setting.											

config dh-group-17

Parameter	Description	Type	Size	Default								
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Use global Diffie-Hellman key pair cache setting.</td></tr><tr><td><i>custom</i></td><td>Use custom Diffie-Hellman key pair cache setting.</td></tr></table>	Option	Description	<i>global</i>	Use global Diffie-Hellman key pair cache setting.	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.					
Option	Description											
<i>global</i>	Use global Diffie-Hellman key pair cache setting.											
<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.											
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0								
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>software</i></td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr><tr><td><i>hardware</i></td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr><tr><td><i>global</i></td><td>Use global dh-mode setting.</td></tr></table>	Option	Description	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.	<i>global</i>	Use global dh-mode setting.			
Option	Description											
<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.											
<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.											
<i>global</i>	Use global dh-mode setting.											

config dh-group-18

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-19

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-2

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		

Parameter	Description	Type	Size	Default								
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0								
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>software</td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr><tr><td>hardware</td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr><tr><td>global</td><td>Use global dh-mode setting.</td></tr></table>				Option	Description	software	Prefer CPU to perform Diffie-Hellman calculations.	hardware	Prefer CPX to perform Diffie-Hellman calculations.	global	Use global dh-mode setting.
Option	Description											
software	Prefer CPU to perform Diffie-Hellman calculations.											
hardware	Prefer CPX to perform Diffie-Hellman calculations.											
global	Use global dh-mode setting.											

config dh-group-20

Parameter	Description	Type	Size	Default								
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Use global Diffie-Hellman key pair cache setting.</td></tr><tr><td><i>custom</i></td><td>Use custom Diffie-Hellman key pair cache setting.</td></tr></table>	Option	Description	<i>global</i>	Use global Diffie-Hellman key pair cache setting.	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.					
Option	Description											
<i>global</i>	Use global Diffie-Hellman key pair cache setting.											
<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.											
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0								
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>software</i></td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr><tr><td><i>hardware</i></td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr><tr><td><i>global</i></td><td>Use global dh-mode setting.</td></tr></table>	Option	Description	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.	<i>global</i>	Use global dh-mode setting.			
Option	Description											
<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.											
<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.											
<i>global</i>	Use global dh-mode setting.											

config dh-group-21

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-27

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-28

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-29

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		

Parameter	Description	Type	Size	Default								
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0								
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>software</td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr><tr><td>hardware</td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr><tr><td>global</td><td>Use global dh-mode setting.</td></tr></table>				Option	Description	software	Prefer CPU to perform Diffie-Hellman calculations.	hardware	Prefer CPX to perform Diffie-Hellman calculations.	global	Use global dh-mode setting.
Option	Description											
software	Prefer CPU to perform Diffie-Hellman calculations.											
hardware	Prefer CPX to perform Diffie-Hellman calculations.											
global	Use global dh-mode setting.											

config dh-group-30

Parameter	Description	Type	Size	Default								
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Use global Diffie-Hellman key pair cache setting.</td></tr><tr><td><i>custom</i></td><td>Use custom Diffie-Hellman key pair cache setting.</td></tr></table>	Option	Description	<i>global</i>	Use global Diffie-Hellman key pair cache setting.	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.					
Option	Description											
<i>global</i>	Use global Diffie-Hellman key pair cache setting.											
<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.											
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0								
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>software</i></td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr><tr><td><i>hardware</i></td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr><tr><td><i>global</i></td><td>Use global dh-mode setting.</td></tr></table>	Option	Description	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.	<i>global</i>	Use global dh-mode setting.			
Option	Description											
<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.											
<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.											
<i>global</i>	Use global dh-mode setting.											

config dh-group-31

Parameter	Description	Type	Size	Default								
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Use global Diffie-Hellman key pair cache setting.</td></tr><tr><td><i>custom</i></td><td>Use custom Diffie-Hellman key pair cache setting.</td></tr></table>	Option	Description	<i>global</i>	Use global Diffie-Hellman key pair cache setting.	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.					
Option	Description											
<i>global</i>	Use global Diffie-Hellman key pair cache setting.											
<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.											
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0								
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>software</i></td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr><tr><td><i>hardware</i></td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr><tr><td><i>global</i></td><td>Use global dh-mode setting.</td></tr></table>	Option	Description	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.	<i>global</i>	Use global dh-mode setting.			
Option	Description											
<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.											
<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.											
<i>global</i>	Use global dh-mode setting.											

config dh-group-32

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config dh-group-5

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

config system interface

Configure interfaces.

```
config system interface
  Description: Configure interfaces.
  edit <name>
    set ac-name {string}
    set aggregate {string}
    set aggregate-type [physical|vxlan]
    set algorithm [L2|L3|...]
```

```

set alias {string}
set allowaccess {option1}, {option2}, ...
set annex [a|b|...]
set ap-discover [enable|disable]
set arpforward [enable|disable]
set atm-protocol [none|ipoa]
set auth-cert {string}
set auth-portal-addr {string}
set auth-type [auto|pap|...]
set auto-auth-extension-device [enable|disable]
set bandwidth-measure-time {integer}
set bfd [global|enable|...]
set bfd-desired-min-tx {integer}
set bfd-detect-mult {integer}
set bfd-required-min-rx {integer}
set broadcast-forward [enable|disable]
set cli-conn-status {integer}
config client-options
    Description: DHCP client options.
    edit <id>
        set code {integer}
        set ip {user}
        set type [hex|string|...]
        set value {string}
    next
end
set color {integer}
set dedicated-to [none|management]
set default-purdue-level [1|1.5|...]
set defaultgw [enable|disable]
set description {var-string}
set detected-peer-mtu {integer}
set detectprotocol {option1}, {option2}, ...
set detectserver {user}
set device-identification [enable|disable]
set device-user-identification [enable|disable]
set devindex {integer}
set dhcp-broadcast-flag [disable|enable]
set dhcp-classless-route-addition [enable|disable]
set dhcp-client-identifier {string}
set dhcp-relay-agent-option [enable|disable]
set dhcp-relay-allow-no-end-option [disable|enable]
set dhcp-relay-circuit-id {string}
set dhcp-relay-interface {string}
set dhcp-relay-interface-select-method [auto|sdwan|...]
set dhcp-relay-ip {user}
set dhcp-relay-link-selection {ipv4-address}
set dhcp-relay-request-all-server [disable|enable]
set dhcp-relay-service [disable|enable]
set dhcp-relay-source-ip {ipv4-address}
set dhcp-relay-type [regular|ipsec]
set dhcp-relay-vrf-select {integer}

```

```

set dhcp-renew-time {integer}
set dhcp-smart-relay [disable|enable]
config dhcp-snooping-server-list
    Description: Configure DHCP server access list.
    edit <name>
        set server-ip {ipv4-address}
    next
end
set disc-retry-timeout {integer}
set distance {integer}
set dns-server-override [enable|disable]
set dns-server-protocol {option1}, {option2}, ...
set drop-fragment [enable|disable]
set eap-ca-cert {string}
set eap-identity {string}
set eap-method [tls|peap]
set eap-password {password}
set eap-supPLICant [enable|disable]
set eap-user-cert {string}
set egress-cos [disable|cos0|...]
config egress-queues
    Description: Configure queues of NP port on egress path.
    set cos0 {string}
    set cos1 {string}
    set cos2 {string}
    set cos3 {string}
    set cos4 {string}
    set cos5 {string}
    set cos6 {string}
    set cos7 {string}
end
set egress-shaping-profile {string}
set eip {ipv4-address-any}
set estimated-downstream-bandwidth {integer}
set estimated-upstream-bandwidth {integer}
set exclude-signatures {option1}, {option2}, ...
set explicit-ftp-proxy [enable|disable]
set explicit-web-proxy [enable|disable]
set external [enable|disable]
set fail-action-on-extender [soft-restart|hard-restart|...]
set fail-alert-interfaces <name1>, <name2>, ...
set fail-alert-method [link-failed-signal|link-down]
set fail-detect [enable|disable]
set fail-detect-option {option1}, {option2}, ...
set fortilink [enable|disable]
set fortilink-backup-link {integer}
set fortilink-neighbor-detect [lldp|fortilink]
set fortilink-split-interface [enable|disable]
set forward-domain {integer}
set forward-error-correction [none|disable|...]
set gateway-address {ipv4-address}
set gwaddr {ipv4-address}

```

```

set gwdetect [enable|disable]
set ha-priority {integer}
set icmp-accept-redirect [enable|disable]
set icmp-send-redirect [enable|disable]
set ident-accept [enable|disable]
set idle-timeout {integer}
set ike-saml-server {string}
set inbandwidth {integer}
set ingress-cos [disable|cos0|...]
set ingress-shaping-profile {string}
set ingress-spillover-threshold {integer}
set interconnect-profile [default|profile1|...]
set interface {string}
set internal {integer}
set ip {ipv4-classnet-host}
set ip-managed-by-fortiipam [inherit-global|enable|...]
set ipmac [enable|disable]
set ips-sniffer-mode [enable|disable]
set ipunnumbered {ipv4-address}
config ipv6
    Description: IPv6 of interface.
    set autoconf [enable|disable]
    set cli-conn6-status {integer}
    config client-options
        Description: DHCP6 client options.
        edit <id>
            set code {integer}
            set ip6 {user}
            set type [hex|string|...]
            set value {string}
        next
    end
    set dhcp6-client-options {option1}, {option2}, ...
    config dhcp6-iapd-list
        Description: DHCPv6 IA-PD list.
        edit <iaid>
            set prefix-hint {ipv6-network}
            set prefix-hint-plt {integer}
            set prefix-hint-vlt {integer}
        next
    end
    set dhcp6-information-request [enable|disable]
    set dhcp6-prefix-delegation [enable|disable]
    set dhcp6-relay-interface-id {string}
    set dhcp6-relay-ip {user}
    set dhcp6-relay-service [disable|enable]
    set dhcp6-relay-source-interface [disable|enable]
    set dhcp6-relay-source-ip {ipv6-address}
    set dhcp6-relay-type {option}
    set icmp6-send-redirect [enable|disable]
    set interface-identifier {ipv6-address}
    set ip6-address {ipv6-prefix}

```

```

set ip6-adv-rio [enable|disable]
set ip6-allowaccess {option1}, {option2}, ...
set ip6-default-life {integer}
set ip6-delegated-prefix-iaid {integer}
config ip6-delegated-prefix-list
    Description: Advertised IPv6 delegated prefix list.
    edit <prefix-id>
        set autonomous-flag [enable|disable]
        set delegated-prefix-iaid {integer}
        set onlink-flag [enable|disable]
        set rdns {user}
        set rdns-service [delegated|default|...]
        set subnet {ipv6-network}
        set upstream-interface {string}
    next
end
set ip6-dns-server-override [enable|disable]
config ip6-dnssl-list
    Description: Advertised IPv6 DNSS list.
    edit <domain>
        set dnssl-life-time {integer}
    next
end
config ip6-extra-addr
    Description: Extra IPv6 address prefixes of interface.
    edit <prefix>
    next
end
set ip6-hop-limit {integer}
set ip6-link-mtu {integer}
set ip6-manage-flag [enable|disable]
set ip6-max-interval {integer}
set ip6-min-interval {integer}
set ip6-mode [static|dhcp|...]
set ip6-other-flag [enable|disable]
config ip6-prefix-list
    Description: Advertised prefix list.
    edit <prefix>
        set autonomous-flag [enable|disable]
        set onlink-flag [enable|disable]
        set preferred-life-time {integer}
        set valid-life-time {integer}
    next
end
set ip6-prefix-mode [dhcp6|ra]
config ip6-rdns-list
    Description: Advertised IPv6 RDNS list.
    edit <rdns>
        set rdns-life-time {integer}
    next
end
set ip6-reachable-time {integer}

```

```

set ip6-retrans-time {integer}
config ip6-route-list
    Description: Advertised route list.
    edit <route>
        set route-life-time {integer}
        set route-pref [medium|high|...]
    next
end
set ip6-route-pref [medium|high|...]
set ip6-send-adv [enable|disable]
set ip6-subnet {ipv6-prefix}
set ip6-upstream-interface {string}
set nd-cert {string}
set nd-cga-modifier {user}
set nd-mode [basic|SEND-compatible]
set nd-security-level {integer}
set nd-timestamp-delta {integer}
set nd-timestamp-fuzz {integer}
set ra-send-mtu [enable|disable]
set unique-autoconf-addr [enable|disable]
set vrip6_link_local {ipv6-address}
set vrrp-virtual-mac6 [enable|disable]
config vrrp6
    Description: IPv6 VRRP configuration.
    edit <vrid>
        set accept-mode [enable|disable]
        set adv-interval {integer}
        set ignore-default-route [enable|disable]
        set preempt [enable|disable]
        set priority {integer}
        set start-time {integer}
        set status [enable|disable]
        set vrdst-priority {integer}
        set vrdst6 {ipv6-address}
        set vrgrp {integer}
        set vrip6 {ipv6-address}
    next
end
end
set l2forward [enable|disable]
set l2tp-client [enable|disable]
config l2tp-client-settings
    Description: L2TP client settings.
    set auth-type [auto|pap|...]
    set defaultgw [enable|disable]
    set distance {integer}
    set hello-interval {integer}
    set ip {ipv4-classnet-host}
    set mtu {integer}
    set password {password}
    set peer-host {string}
    set peer-mask {ipv4-netmask}

```

```

        set peer-port {integer}
        set priority {integer}
        set user {string}
    end
    set lacp-ha-secondary [enable|disable]
    set lacp-mode [static|passive|...]
    set lacp-speed [slow|fast]
    set lcp-echo-interval {integer}
    set lcp-max-echo-fails {integer}
    set link-up-delay {integer}
    set lldp-network-policy {string}
    set lldp-reception [enable|disable|...]
    set lldp-transmission [enable|disable|...]
    set macaddr {mac-address}
    set managed-subnetwork-size [4|8|...]
    set management-ip {ipv4-classnet-host}
    set measured-downstream-bandwidth {integer}
    set measured-upstream-bandwidth {integer}
    set mediatype [serdes-sfp|sgmii-sfp|...]
    set member <interface-name1>, <interface-name2>, ...
    set min-links {integer}
    set min-links-down [operational|administrative]
    set mirroring-direction [rx|tx|...]
    config mirroring-filter
        Description: Mirroring filter.
        set filter-dport {integer}
        set filter-dstip {ipv4-classnet-host}
        set filter-protocol {integer}
        set filter-sport {integer}
        set filter-srcip {ipv4-classnet-host}
    end
    set mirroring-port {string}
    set mode [static|dhcp|...]
    set monitor-bandwidth [enable|disable]
    set mtu {integer}
    set mtu-override [enable|disable]
    set mux-type [llc-encaps|vc-encaps]
    set ndiscforward [enable|disable]
    set netbios-forward [disable|enable]
    set netflow-sample-rate {integer}
    set netflow-sampler [disable|tx|...]
    set netflow-sampler-id {integer}
    set np-qos-profile {integer}
    set outbandwidth {integer}
    set padt-retry-timeout {integer}
    set password {password}
    set phy-mode {option}
    set ping-serv-status {integer}
    set poe [enable|disable]
    set polling-interval {integer}
    set port-mirroring [disable|enable]
    set pppoe-egress-cos [cos0|cos1|...]

```



```

set pppoe-unnumbered-negotiate [enable|disable]
set pptp-auth-type [auto|pap|...]
set pptp-client [enable|disable]
set pptp-password {password}
set pptp-server-ip {ipv4-address}
set pptp-timeout {integer}
set pptp-user {string}
set preserve-session-route [enable|disable]
set priority {integer}
set priority-override [enable|disable]
set proxy-captive-portal [enable|disable]
set pvc-atm-qos [cbr|rt-vbr|...]
set pvc-chan {integer}
set pvc-crc {integer}
set pvc-pcr {integer}
set pvc-scr {integer}
set pvc-vlan-id {integer}
set pvc-vlan-rx-id {integer}
set pvc-vlan-rx-op [pass-through|replace|...]
set pvc-vlan-tx-id {integer}
set pvc-vlan-tx-op [pass-through|replace|...]
set reachable-time {integer}
set redundant-interface {string}
set remote-ip {ipv4-classnet-host}
set replacemsg-override-group {string}
set retransmission [disable|enable]
set ring-rx {integer}
set ring-tx {integer}
set role [lan|wan|...]
set sample-direction [tx|rx|...]
set sample-rate {integer}
set secondary-IP [enable|disable]
config secondaryip
    Description: Second IP address of interface.
    edit <id>
        set allowaccess {option1}, {option2}, ...
        set detectprotocol {option1}, {option2}, ...
        set detectserver {user}
        set gwdetect [enable|disable]
        set ha-priority {integer}
        set ip {ipv4-classnet-host}
        set ping-serv-status {integer}
        set secip-relay-ip {user}
    next
end
set security-8021x-dynamic-vlan-id {integer}
set security-8021x-master {string}
set security-8021x-member-mode [switch|disable]
set security-8021x-mode [default|dynamic-vlan|...]
set security-exempt-list {string}
set security-external-logout {string}
set security-external-web {var-string}

```

```

set security-groups <name1>, <name2>, ...
set security-ip-auth-bypass [enable|disable]
set security-mac-auth-bypass [mac-auth-only|enable|...]
set security-mode [none|captive-portal|...]
set security-redirect-url {var-string}
set select-profile-30a-35b [30A|35B]
set service-name {string}
set sflow-sampler [enable|disable]
set sfp-dsl [disable|enable]
set sfp-dsl-adsl-fallback [disable|enable]
set sfp-dsl-autodetect [disable|enable]
set sfp-dsl-mac {mac-address}
set snmp-index {integer}
set speed [auto|10full|...]
set spillover-threshold {integer}
set src-check [enable|disable]
set status [up|down]
set stp [disable|enable]
set stp-edge [disable|enable]
set stp-ha-secondary [disable|enable|...]
set stpforward [enable|disable]
set stpforward-mode [rpl-all-ext-id|rpl-bridge-ext-id|...]
set subst [enable|disable]
set substitute-dst-mac {mac-address}
set sw-algorithm [12|13|...]
set swc-first-create {integer}
set swc-vlan {integer}
set switch {string}
set switch-controller-access-vlan [enable|disable]
set switch-controller-arp-inspection [enable|disable|...]
set switch-controller-dhcp-snooping [enable|disable]
set switch-controller-dhcp-snooping-option82 [enable|disable]
set switch-controller-dhcp-snooping-verify-mac [enable|disable]
set switch-controller-dynamic {string}
set switch-controller-feature [none|default-vlan|...]
set switch-controller-igmp-snooping [enable|disable]
set switch-controller-igmp-snooping-fast-leave [enable|disable]
set switch-controller-igmp-snooping-proxy [enable|disable]
set switch-controller-iot-scanning [enable|disable]
set switch-controller-learning-limit {integer}
set switch-controller-mgmt-vlan {integer}
set switch-controller-nac {string}
set switch-controller-netflow-collect [disable|enable]
set switch-controller-offload [enable|disable]
set switch-controller-offload-gw [enable|disable]
set switch-controller-offload-ip {ipv4-address}
set switch-controller-rspan-mode [disable|enable]
set switch-controller-source-ip [outbound|fixed]
set switch-controller-traffic-policy {string}
set system-id {mac-address}
set system-id-type [auto|user]
config tagging

```

```

    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set tc-mode {option}
set tcp-mss {integer}
set telemetry-discover [enable|disable]
set trunk [enable|disable]
set trust-ip-1 {ipv4-classnet-any}
set trust-ip-2 {ipv4-classnet-any}
set trust-ip-3 {ipv4-classnet-any}
set trust-ip6-1 {ipv6-prefix}
set trust-ip6-2 {ipv6-prefix}
set trust-ip6-3 {ipv6-prefix}
set type [physical|vlan|...]
set username {string}
set vci {integer}
set vdom {string}
set vectoring [disable|enable]
set vindex {integer}
set virtual-mac {mac-address}
set vlan-id {integer}
set vlan-op-mode [tag|untag|...]
set vlan-protocol [8021q|8021ad]
set vlanforward [enable|disable]
set vlanid {integer}
set vpi {integer}
set vrf {integer}
config vrrp
    Description: VRRP configuration.
    edit <vrid>
        set accept-mode [enable|disable]
        set adv-interval {integer}
        set ignore-default-route [enable|disable]
        set preempt [enable|disable]
        set priority {integer}
        config proxy-arp
            Description: VRRP Proxy ARP configuration.
            edit <id>
                set ip {user}
            next
        end
        set start-time {integer}
        set status [enable|disable]
        set version [2|3]
        set vrdst {ipv4-address-any}
        set vrdst-priority {integer}
        set vrgrp {integer}
        set vrip {ipv4-address-any}
    next

```

```

end
set vrrp-virtual-mac [enable|disable]
set wccp [enable|disable]
set weight {integer}
set wifi-5g-threshold {string}
set wifi-acl [allow|deny]
set wifi-ap-band [any|5g-preferred|...]
set wifi-auth [PSK|radius|...]
set wifi-auto-connect [enable|disable]
set wifi-auto-save [enable|disable]
set wifi-broadcast-ssid [enable|disable]
set wifi-dns-server1 {ipv4-address}
set wifi-dns-server2 {ipv4-address}
set wifi-encrypt [TKIP|AES]
set wifi-fragment-threshold {integer}
set wifi-gateway {ipv4-address}
set wifi-key {password}
set wifi-keyindex {integer}
set wifi-mac-filter [enable|disable]
config wifi-mac-list
    Description: MAC filter list.
    edit <id>
        set mac {mac-address}
    next
end
config wifi-networks
    Description: WiFi network table.
    edit <id>
        set wifi-ca-certificate {string}
        set wifi-client-certificate {string}
        set wifi-eap-type [both|tls|...]
        set wifi-encrypt [TKIP|AES]
        set wifi-key {password}
        set wifi-keyindex {integer}
        set wifi-passphrase {password}
        set wifi-private-key {string}
        set wifi-private-key-password {password}
        set wifi-security [open|wep64|...]
        set wifi-ssid {string}
        set wifi-username {string}
    next
end
set wifi-passphrase {password}
set wifi-radius-server {string}
set wifi-rts-threshold {integer}
set wifi-security [open|wep64|...]
set wifi-ssid {string}
set wifi-usergroup {string}
set wins-ip {ipv4-address}
next
end

```

config system interface

Parameter	Description	Type	Size	Default																		
ac-name	PPPoE server name.	string	Maximum length: 63																			
aggregate	Aggregate interface. Read-only.	string	Maximum length: 15																			
aggregate-type	Type of aggregation.	option	-	physical																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>physical</i></td><td>Physical interface aggregation.</td></tr><tr><td><i>vxlان</i></td><td>VXLAN interface aggregation.</td></tr></table>	Option	Description	<i>physical</i>	Physical interface aggregation.	<i>vxlان</i>	VXLAN interface aggregation.															
Option	Description																					
<i>physical</i>	Physical interface aggregation.																					
<i>vxlان</i>	VXLAN interface aggregation.																					
algorithm	Frame distribution algorithm.	option	-	L4																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>L2</i></td><td>Use layer 2 address for distribution.</td></tr><tr><td><i>L3</i></td><td>Use layer 3 address for distribution.</td></tr><tr><td><i>L4</i></td><td>Use layer 4 information for distribution.</td></tr><tr><td><i>Source-MAC</i></td><td>Use source MAC address for distribution.</td></tr></table>	Option	Description	<i>L2</i>	Use layer 2 address for distribution.	<i>L3</i>	Use layer 3 address for distribution.	<i>L4</i>	Use layer 4 information for distribution.	<i>Source-MAC</i>	Use source MAC address for distribution.											
Option	Description																					
<i>L2</i>	Use layer 2 address for distribution.																					
<i>L3</i>	Use layer 3 address for distribution.																					
<i>L4</i>	Use layer 4 information for distribution.																					
<i>Source-MAC</i>	Use source MAC address for distribution.																					
alias	Alias will be displayed with the interface name to make it easier to distinguish.	string	Maximum length: 25																			
allowaccess	Permitted types of management access to this interface.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>fgfm</i></td><td>FortiManager access.</td></tr><tr><td><i>radius-acct</i></td><td>RADIUS accounting access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.			
Option	Description																					
<i>ping</i>	PING access.																					
<i>https</i>	HTTPS access.																					
<i>ssh</i>	SSH access.																					
<i>snmp</i>	SNMP access.																					
<i>http</i>	HTTP access.																					
<i>telnet</i>	TELNET access.																					
<i>fgfm</i>	FortiManager access.																					
<i>radius-acct</i>	RADIUS accounting access.																					

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>probe-response</i></td><td>Probe access.</td></tr><tr><td><i>fabric</i></td><td>Security Fabric access.</td></tr><tr><td><i>ftm</i></td><td>FTM access.</td></tr><tr><td><i>speed-test</i></td><td>Speed test access.</td></tr><tr><td><i>scim</i></td><td>System for Cross-domain Identity Management (SCIM) access.</td></tr></table>	Option	Description	<i>probe-response</i>	Probe access.	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.	<i>speed-test</i>	Speed test access.	<i>scim</i>	System for Cross-domain Identity Management (SCIM) access.									
	Option	Description																				
	<i>probe-response</i>	Probe access.																				
	<i>fabric</i>	Security Fabric access.																				
	<i>ftm</i>	FTM access.																				
	<i>speed-test</i>	Speed test access.																				
<i>scim</i>	System for Cross-domain Identity Management (SCIM) access.																					
annex *	Configure xDSL annex type.	option	-	a																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>a</i></td><td>xDSL Annex A</td></tr><tr><td><i>b</i></td><td>xDSL Annex B</td></tr><tr><td><i>j</i></td><td>xDSL Annex J</td></tr><tr><td><i>bjm</i></td><td>xDSL Annex BJM</td></tr><tr><td><i>i</i></td><td>xDSL Annex I</td></tr><tr><td><i>al</i></td><td>xDSL Annex AL</td></tr><tr><td><i>m</i></td><td>xDSL Annex M</td></tr><tr><td><i>aijlm</i></td><td>xDSL Annex AIJLM</td></tr></table>	Option	Description	<i>a</i>	xDSL Annex A	<i>b</i>	xDSL Annex B	<i>j</i>	xDSL Annex J	<i>bjm</i>	xDSL Annex BJM	<i>i</i>	xDSL Annex I	<i>al</i>	xDSL Annex AL	<i>m</i>	xDSL Annex M	<i>aijlm</i>	xDSL Annex AIJLM			
	Option	Description																				
	<i>a</i>	xDSL Annex A																				
	<i>b</i>	xDSL Annex B																				
	<i>j</i>	xDSL Annex J																				
	<i>bjm</i>	xDSL Annex BJM																				
	<i>i</i>	xDSL Annex I																				
	<i>al</i>	xDSL Annex AL																				
<i>m</i>	xDSL Annex M																					
<i>aijlm</i>	xDSL Annex AIJLM																					
ap-discover	Enable/disable automatic registration of unknown FortiAP devices.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic registration of unknown FortiAP devices.</td></tr><tr><td><i>disable</i></td><td>Disable automatic registration of unknown FortiAP devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic registration of unknown FortiAP devices.	<i>disable</i>	Disable automatic registration of unknown FortiAP devices.															
	Option	Description																				
	<i>enable</i>	Enable automatic registration of unknown FortiAP devices.																				
<i>disable</i>	Disable automatic registration of unknown FortiAP devices.																					
arpforward	Enable/disable ARP forwarding.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ARP forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable ARP forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable ARP forwarding.	<i>disable</i>	Disable ARP forwarding.															
	Option	Description																				
	<i>enable</i>	Enable ARP forwarding.																				
<i>disable</i>	Disable ARP forwarding.																					
atm-protocol *	ATM protocol.	option	-	none																		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Not over ATM.</td></tr><tr><td><i>ipoa</i></td><td>IPoA RFC2684.</td></tr></table>	Option	Description	<i>none</i>	Not over ATM.	<i>ipoa</i>	IPoA RFC2684.									
	Option	Description														
	<i>none</i>	Not over ATM.														
<i>ipoa</i>	IPoA RFC2684.															
auth-cert	HTTPS server certificate.	string	Maximum length: 35													
auth-portal-addr	Address of captive portal.	string	Maximum length: 63													
auth-type	PPP authentication type to use.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically choose authentication.</td></tr><tr><td><i>pap</i></td><td>PAP authentication.</td></tr><tr><td><i>chap</i></td><td>CHAP authentication.</td></tr><tr><td><i>mschapv1</i></td><td>MS-CHAPv1 authentication.</td></tr><tr><td><i>mschapv2</i></td><td>MS-CHAPv2 authentication.</td></tr></table>	Option	Description	<i>auto</i>	Automatically choose authentication.	<i>pap</i>	PAP authentication.	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.			
	Option	Description														
	<i>auto</i>	Automatically choose authentication.														
	<i>pap</i>	PAP authentication.														
	<i>chap</i>	CHAP authentication.														
	<i>mschapv1</i>	MS-CHAPv1 authentication.														
<i>mschapv2</i>	MS-CHAPv2 authentication.															
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension device on this interface.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic authorization of dedicated Fortinet extension device on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable automatic authorization of dedicated Fortinet extension device on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device on this interface.	<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device on this interface.									
	Option	Description														
	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device on this interface.														
<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device on this interface.															
bandwidth-measure-time	Bandwidth measure time.	integer	Minimum value: 0 0 Maximum value: 4294967295													
bfd	Bidirectional Forwarding Detection (BFD) settings.	option	-	global												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>BFD behavior of this interface will be based on global configuration.</td></tr><tr><td><i>enable</i></td><td>Enable BFD on this interface and ignore global configuration.</td></tr><tr><td><i>disable</i></td><td>Disable BFD on this interface and ignore global configuration.</td></tr></table>	Option	Description	<i>global</i>	BFD behavior of this interface will be based on global configuration.	<i>enable</i>	Enable BFD on this interface and ignore global configuration.	<i>disable</i>	Disable BFD on this interface and ignore global configuration.							
	Option	Description														
	<i>global</i>	BFD behavior of this interface will be based on global configuration.														
	<i>enable</i>	Enable BFD on this interface and ignore global configuration.														
<i>disable</i>	Disable BFD on this interface and ignore global configuration.															

Parameter	Description	Type	Size	Default
bfd-desired-min-tx	BFD desired minimal transmit interval.	integer	Minimum value: 1 Maximum value: 100000	250
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 1 Maximum value: 50	3
bfd-required-min-rx	BFD required minimal receive interval.	integer	Minimum value: 1 Maximum value: 100000	250
broadcast-forward	Enable/disable broadcast forwarding.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable broadcast forwarding.		
	<i>disable</i>	Disable broadcast forwarding.		
cli-conn-status	CLI connection status. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
dedicated-to	Configure interface for single purpose.	option	-	none
	Option	Description		
	<i>none</i>	Interface not dedicated for any purpose.		
	<i>management</i>	Dedicate this interface for management purposes only.		
default-purdue-level	default purdue level of device detected on this interface.	option	-	3
	Option	Description		
	<i>1</i>	Level 1 - Basic Control		
	<i>1.5</i>	Level 1.5		
	<i>2</i>	Level 2 - Area Supervisory Control		
	<i>2.5</i>	Level 2.5		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>3</td><td>Level 3 - Operations & Control</td></tr><tr><td>3.5</td><td>Level 3.5</td></tr><tr><td>4</td><td>Level 4 - Business Planning & Logistics</td></tr><tr><td>5</td><td>Level 5 - Enterprise Network</td></tr><tr><td>5.5</td><td>Level 5.5</td></tr></table>	Option	Description	3	Level 3 - Operations & Control	3.5	Level 3.5	4	Level 4 - Business Planning & Logistics	5	Level 5 - Enterprise Network	5.5	Level 5.5			
	Option	Description														
	3	Level 3 - Operations & Control														
	3.5	Level 3.5														
	4	Level 4 - Business Planning & Logistics														
	5	Level 5 - Enterprise Network														
5.5	Level 5.5															
defaultgw	Enable to get the gateway IP from the DHCP or PPPoE server.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable default gateway.</td></tr><tr><td>disable</td><td>Disable default gateway.</td></tr></table>	Option	Description	enable	Enable default gateway.	disable	Disable default gateway.									
	Option	Description														
	enable	Enable default gateway.														
disable	Disable default gateway.															
description	Description.	var-string	Maximum length: 255													
detected-peer-mtu	MTU of detected peer (0 - 4294967295). Read-only.	integer	Minimum value: 0 Maximum value: 4294967295													
detectprotocol	Protocols used to detect the server.	option	-	ping												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING.</td></tr><tr><td>tcp-echo</td><td>TCP echo.</td></tr><tr><td>udp-echo</td><td>UDP echo.</td></tr></table>	Option	Description	ping	PING.	tcp-echo	TCP echo.	udp-echo	UDP echo.							
	Option	Description														
	ping	PING.														
	tcp-echo	TCP echo.														
udp-echo	UDP echo.															
detectserver	Gateway's ping server for this IP.	user	Not Specified													
device-identification	Enable/disable passively gathering of device identity information about the devices on the network connected to this interface.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable passive gathering of identity information about hosts.</td></tr><tr><td>disable</td><td>Disable passive gathering of identity information about hosts.</td></tr></table>	Option	Description	enable	Enable passive gathering of identity information about hosts.	disable	Disable passive gathering of identity information about hosts.									
	Option	Description														
	enable	Enable passive gathering of identity information about hosts.														
disable	Disable passive gathering of identity information about hosts.															

Parameter	Description	Type	Size	Default						
device-user-identification	Enable/disable passive gathering of user identity information about users on this interface.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable passive gathering of user identity information about users.</td></tr><tr><td><i>disable</i></td><td>Disable passive gathering of user identity information about users.</td></tr></table>	Option	Description	<i>enable</i>	Enable passive gathering of user identity information about users.	<i>disable</i>	Disable passive gathering of user identity information about users.			
Option	Description									
<i>enable</i>	Enable passive gathering of user identity information about users.									
<i>disable</i>	Disable passive gathering of user identity information about users.									
devindex	Device Index. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							
dhcp-broadcast-flag	Enable/disable setting of the broadcast flag in messages sent by the DHCP client (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable broadcast flag.</td></tr><tr><td><i>enable</i></td><td>Enable broadcast flag.</td></tr></table>	Option	Description	<i>disable</i>	Disable broadcast flag.	<i>enable</i>	Enable broadcast flag.			
Option	Description									
<i>disable</i>	Disable broadcast flag.									
<i>enable</i>	Enable broadcast flag.									
dhcp-classless-route-addition	Enable/disable addition of classless static routes retrieved from DHCP server.	option	-	disable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable addition of classless static routes retrieved from DHCP server.</td></tr><tr><td><i>disable</i></td><td>Disable addition of classless static routes retrieved from DHCP server.</td></tr></table>	Option	Description	<i>enable</i>	Enable addition of classless static routes retrieved from DHCP server.	<i>disable</i>	Disable addition of classless static routes retrieved from DHCP server.			
Option	Description									
<i>enable</i>	Enable addition of classless static routes retrieved from DHCP server.									
<i>disable</i>	Disable addition of classless static routes retrieved from DHCP server.									
dhcp-client-identifier	DHCP client identifier.	string	Maximum length: 48							
dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP relay agent option.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP relay agent option.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP relay agent option.	<i>disable</i>	Disable DHCP relay agent option.			
Option	Description									
<i>enable</i>	Enable DHCP relay agent option.									
<i>disable</i>	Disable DHCP relay agent option.									
dhcp-relay-allow-no-end-option	Enable/disable relaying DHCP messages with no end option.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable relaying DHCP messages with no end option.		
	<i>enable</i>	Enable relaying DHCP messages with no end option.		
dhcp-relay-circuit-id	DHCP relay circuit ID.	string	Maximum length: 64	
dhcp-relay-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
dhcp-relay-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option Description			
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
dhcp-relay-ip	DHCP relay IP address.	user	Not Specified	
dhcp-relay-link-selection	DHCP relay link selection.	ipv4-address	Not Specified	0.0.0.0
dhcp-relay-request-all-server	Enable/disable sending of DHCP requests to all servers.	option	-	disable
	Option Description			
	<i>disable</i>	Send DHCP requests only to a matching server.		
	<i>enable</i>	Send DHCP requests to all servers.		
dhcp-relay-service	Enable/disable allowing this interface to act as a DHCP relay.	option	-	disable
	Option Description			
	<i>disable</i>	None.		
	<i>enable</i>	DHCP relay agent.		
dhcp-relay-source-ip	IP address used by the DHCP relay as its source IP.	ipv4-address	Not Specified	0.0.0.0
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-	regular

Parameter	Description	Type	Size	Default
	Option Description			
	<i>regular</i>	Regular DHCP relay.		
	<i>ipsec</i>	DHCP relay for IPsec.		
dhcp-relay-vrf-select	VRF ID used for connection to server.	integer	Minimum value: -1 0 Maximum value: 511	
dhcp-renew-time	DHCP renew time in seconds (300-604800), 0 means use the renew time provided by the server.	integer	Minimum value: 0 300 Maximum value: 604800	
dhcp-smart-relay	Enable/disable DHCP smart relay.	option	-	disable
	Option Description			
	<i>disable</i>	Disable DHCP smart relay.		
	<i>enable</i>	Enable DHCP smart relay.		
disc-retry-timeout	Time in seconds to wait before retrying to start a PPPoE discovery, 0 means no timeout.	integer	Minimum value: 1 0 Maximum value: 4294967295	
distance	Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route.	integer	Minimum value: 5 1 Maximum value: 255	
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-	enable
	Option Description			
	<i>enable</i>	Use DNS acquired by DHCP or PPPoE.		
	<i>disable</i>	No not use DNS acquired by DHCP or PPPoE.		
dns-server-protocol	DNS transport protocols.	option	-	cleartext
	Option Description			
	<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.		
	<i>dot</i>	DNS over TLS/853.		
	<i>doh</i>	DNS over HTTPS/443.		

Parameter	Description	Type	Size	Default
drop-fragment	Enable/disable drop fragment packets.	option	-	disable
	Option Description			
	<i>enable</i>	Enable/disable drop fragment packets.		
	<i>disable</i>	Do not drop fragment packets.		
eap-ca-cert	EAP CA certificate name.	string	Maximum length: 79	
eap-identity	EAP identity.	string	Maximum length: 35	
eap-method	EAP method.	option	-	
	Option Description			
	<i>tls</i>	TLS.		
	<i>peap</i>	PEAP.		
eap-password	EAP password.	password	Not Specified	
eap-suppliant	Enable/disable EAP-Suppliant.	option	-	disable
	Option Description			
	<i>enable</i>	Enable EAP Suppliant.		
	<i>disable</i>	Disable EAP Suppliant.		
eap-user-cert	EAP user certificate name.	string	Maximum length: 35	
egress-cos *	Override outgoing CoS in user VLAN tag.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>cos0</i>	CoS 0.		
	<i>cos1</i>	CoS 1.		
	<i>cos2</i>	CoS 2.		
	<i>cos3</i>	CoS 3.		
	<i>cos4</i>	CoS 4.		
	<i>cos5</i>	CoS 5.		

Parameter	Description	Type	Size	Default
	Option	Description		
	cos6	CoS 6.		
	cos7	CoS 7.		
egress-shaping-profile	Outgoing traffic shaping profile.	string	Maximum length: 35	
eip *	External IP. Read-only.	ipv4-address-any	Not Specified	0.0.0.0
estimated-downstream-bandwidth	Estimated maximum downstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 0 Maximum value: 4294967295	
estimated-upstream-bandwidth	Estimated maximum upstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 0 Maximum value: 4294967295	
exclude-signatures	Exclude IOT or OT application signatures.	option	-	
	Option	Description		
	iot	Exclude IOT appctrl signatures.		
	ot	Exclude OT appctrl signatures.		
explicit-ftp-proxy	Enable/disable the explicit FTP proxy on this interface.	option	-	disable
	Option	Description		
	enable	Enable explicit FTP proxy on this interface.		
	disable	Disable explicit FTP proxy on this interface.		
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-	disable
	Option	Description		
	enable	Enable explicit Web proxy on this interface.		
	disable	Disable explicit Web proxy on this interface.		

Parameter	Description	Type	Size	Default								
external	Enable/disable identifying the interface as an external interface (which usually means it's connected to the Internet).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identifying the interface as an external interface.</td></tr><tr><td><i>disable</i></td><td>Disable identifying the interface as an external interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable identifying the interface as an external interface.	<i>disable</i>	Disable identifying the interface as an external interface.					
Option	Description											
<i>enable</i>	Enable identifying the interface as an external interface.											
<i>disable</i>	Disable identifying the interface as an external interface.											
fail-action-on-extender	Action on FortiExtender when interface fail.	option	-	soft-restart								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>soft-restart</i></td><td>Soft-restart-on-extender.</td></tr><tr><td><i>hard-restart</i></td><td>Hard-restart-on-extender.</td></tr><tr><td><i>reboot</i></td><td>Reboot-on-extender.</td></tr></table>	Option	Description	<i>soft-restart</i>	Soft-restart-on-extender.	<i>hard-restart</i>	Hard-restart-on-extender.	<i>reboot</i>	Reboot-on-extender.			
Option	Description											
<i>soft-restart</i>	Soft-restart-on-extender.											
<i>hard-restart</i>	Hard-restart-on-extender.											
<i>reboot</i>	Reboot-on-extender.											
fail-alert-interfaces <name>	Names of the FortiGate interfaces to which the link failure alert is sent. Names of the non-virtual interface.	string	Maximum length: 15									
fail-alert-method	Select link-failed-signal or link-down method to alert about a failed link.	option	-	link-down								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>link-failed-signal</i></td><td>Link-failed-signal.</td></tr><tr><td><i>link-down</i></td><td>Link-down.</td></tr></table>	Option	Description	<i>link-failed-signal</i>	Link-failed-signal.	<i>link-down</i>	Link-down.					
Option	Description											
<i>link-failed-signal</i>	Link-failed-signal.											
<i>link-down</i>	Link-down.											
fail-detect	Enable/disable fail detection features for this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable interface failed option status.</td></tr><tr><td><i>disable</i></td><td>Disable interface failed option status.</td></tr></table>	Option	Description	<i>enable</i>	Enable interface failed option status.	<i>disable</i>	Disable interface failed option status.					
Option	Description											
<i>enable</i>	Enable interface failed option status.											
<i>disable</i>	Disable interface failed option status.											
fail-detect-option	Options for detecting that this interface has failed.	option	-	link-down								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>detectserver</i></td><td>Use a ping server to determine if the interface has failed.</td></tr><tr><td><i>link-down</i></td><td>Use port detection to determine if the interface has failed.</td></tr></table>	Option	Description	<i>detectserver</i>	Use a ping server to determine if the interface has failed.	<i>link-down</i>	Use port detection to determine if the interface has failed.			
	Option	Description								
	<i>detectserver</i>	Use a ping server to determine if the interface has failed.								
<i>link-down</i>	Use port detection to determine if the interface has failed.									
fortilink *	Enable FortiLink to dedicate this interface to manage other Fortinet devices.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiLink to dedicated interface for managing FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable FortiLink to dedicated interface for managing FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiLink to dedicated interface for managing FortiSwitch devices.	<i>disable</i>	Disable FortiLink to dedicated interface for managing FortiSwitch devices.			
	Option	Description								
	<i>enable</i>	Enable FortiLink to dedicated interface for managing FortiSwitch devices.								
<i>disable</i>	Disable FortiLink to dedicated interface for managing FortiSwitch devices.									
fortilink-backup-link	FortiLink split interface backup link. Read-only.	integer	Minimum value: 0 0 Maximum value: 255							
fortilink-neighbor-detect	Protocol for FortiGate neighbor discovery.	option	-	lldp						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lldp</i></td><td>Detect FortiLink neighbors using LLDP protocol.</td></tr><tr><td><i>fortilink</i></td><td>Detect FortiLink neighbors using FortiLink protocol.</td></tr></table>	Option	Description	<i>lldp</i>	Detect FortiLink neighbors using LLDP protocol.	<i>fortilink</i>	Detect FortiLink neighbors using FortiLink protocol.			
	Option	Description								
	<i>lldp</i>	Detect FortiLink neighbors using LLDP protocol.								
<i>fortilink</i>	Detect FortiLink neighbors using FortiLink protocol.									
fortilink-split-interface	Enable/disable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.</td></tr><tr><td><i>disable</i></td><td>Disable FortiLink split interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	<i>disable</i>	Disable FortiLink split interface.			
	Option	Description								
	<i>enable</i>	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.								
<i>disable</i>	Disable FortiLink split interface.									
forward-domain	Transparent mode forward domain.	integer	Minimum value: 0 0 Maximum value: 2147483647							
forward-error-correction *	Enable/disable forward error correction (FEC).	option	-	none						

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>none</td></tr><tr><td><i>disable</i></td><td>Disable forward error correction (FEC).</td></tr><tr><td><i>cl91-rs-fec</i></td><td>Reed-Solomon (FEC CL91).</td></tr><tr><td><i>cl74-fc-fec</i></td><td>Fire-Code (FEC CL74).</td></tr><tr><td><i>rs-fec544</i></td><td>Reed-Solomon(544, 514).</td></tr><tr><td><i>auto</i></td><td>Negotiate forward error correction (FEC).</td></tr></table>	Option	Description	<i>none</i>	none	<i>disable</i>	Disable forward error correction (FEC).	<i>cl91-rs-fec</i>	Reed-Solomon (FEC CL91).	<i>cl74-fc-fec</i>	Fire-Code (FEC CL74).	<i>rs-fec544</i>	Reed-Solomon(544, 514).	<i>auto</i>	Negotiate forward error correction (FEC).			
	Option	Description																
	<i>none</i>	none																
	<i>disable</i>	Disable forward error correction (FEC).																
	<i>cl91-rs-fec</i>	Reed-Solomon (FEC CL91).																
	<i>cl74-fc-fec</i>	Fire-Code (FEC CL74).																
	<i>rs-fec544</i>	Reed-Solomon(544, 514).																
<i>auto</i>	Negotiate forward error correction (FEC).																	
gateway-address *	Gateway address.	ipv4-address	Not Specified	0.0.0.0														
gwaddr *	Gateway address.	ipv4-address	Not Specified	0.0.0.0														
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable detect gateway alive for first.</td></tr><tr><td><i>disable</i></td><td>Disable detect gateway alive for first.</td></tr></table>	Option	Description	<i>enable</i>	Enable detect gateway alive for first.	<i>disable</i>	Disable detect gateway alive for first.											
	Option	Description																
	<i>enable</i>	Enable detect gateway alive for first.																
<i>disable</i>	Disable detect gateway alive for first.																	
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50															
icmp-accept-redirect	Enable/disable ICMP accept redirect.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ICMP accept redirect.</td></tr><tr><td><i>disable</i></td><td>Disable ICMP accept redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable ICMP accept redirect.	<i>disable</i>	Disable ICMP accept redirect.											
	Option	Description																
	<i>enable</i>	Enable ICMP accept redirect.																
<i>disable</i>	Disable ICMP accept redirect.																	
icmp-send-redirect	Enable/disable sending of ICMP redirects.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of ICMP redirects.</td></tr><tr><td><i>disable</i></td><td>Disable sending of ICMP redirects.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of ICMP redirects.	<i>disable</i>	Disable sending of ICMP redirects.											
	Option	Description																
	<i>enable</i>	Enable sending of ICMP redirects.																
<i>disable</i>	Disable sending of ICMP redirects.																	
ident-accept	Enable/disable authentication for this interface.	option	-	disable														

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable determining a user's identity from packet identification.</td></tr><tr><td><i>disable</i></td><td>Disable determining a user's identity from packet identification.</td></tr></table>	Option	Description	<i>enable</i>	Enable determining a user's identity from packet identification.	<i>disable</i>	Disable determining a user's identity from packet identification.																	
	Option	Description																						
	<i>enable</i>	Enable determining a user's identity from packet identification.																						
<i>disable</i>	Disable determining a user's identity from packet identification.																							
idle-timeout	PPPoE auto disconnect after idle timeout seconds, 0 means no timeout.	integer	Minimum value: 0 0 Maximum value: 32767																					
ike-saml-server	Configure IKE authentication SAML server.	string	Maximum length: 35																					
inbandwidth	Bandwidth limit for incoming traffic (0 - 80000000 kbps), 0 means unlimited.	integer	Minimum value: 0 0 Maximum value: 80000000 **																					
ingress-cos *	Override incoming CoS in user VLAN tag on VLAN interface or assign a priority VLAN tag on physical interface.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>cos0</i></td><td>CoS 0.</td></tr><tr><td><i>cos1</i></td><td>CoS 1.</td></tr><tr><td><i>cos2</i></td><td>CoS 2.</td></tr><tr><td><i>cos3</i></td><td>CoS 3.</td></tr><tr><td><i>cos4</i></td><td>CoS 4.</td></tr><tr><td><i>cos5</i></td><td>CoS 5.</td></tr><tr><td><i>cos6</i></td><td>CoS 6.</td></tr><tr><td><i>cos7</i></td><td>CoS 7.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>cos0</i>	CoS 0.	<i>cos1</i>	CoS 1.	<i>cos2</i>	CoS 2.	<i>cos3</i>	CoS 3.	<i>cos4</i>	CoS 4.	<i>cos5</i>	CoS 5.	<i>cos6</i>	CoS 6.	<i>cos7</i>	CoS 7.			
	Option	Description																						
	<i>disable</i>	Disable.																						
	<i>cos0</i>	CoS 0.																						
	<i>cos1</i>	CoS 1.																						
	<i>cos2</i>	CoS 2.																						
	<i>cos3</i>	CoS 3.																						
	<i>cos4</i>	CoS 4.																						
	<i>cos5</i>	CoS 5.																						
	<i>cos6</i>	CoS 6.																						
<i>cos7</i>	CoS 7.																							
ingress-shaping-profile	Incoming traffic shaping profile.	string	Maximum length: 35																					
ingress-spillover-threshold	Ingress Spillover threshold (0 - 16776000 kbps), 0 means unlimited.	integer	Minimum value: 0 0 Maximum value: 16776000																					
interconnect-profile *	Set interconnect profile.	option	-	default																				

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	default interconnect profile		
	<i>profile1</i>	interconnect profile1 [(10G & IC > 7m/20db-loss) or (25G/27G & IC < 1m)]		
	<i>profile2</i>	interconnect profile2 [(27G in AP (106G) Auto Profile)]		
interface	Interface name.	string	Maximum length: 15	
internal	Implicitly created.	integer	Minimum value: 0 0 Maximum value: 255	
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
ip-managed-by-fortiipam	Enable/disable automatic IP address assignment of this interface by FortiIPAM.	option	-	inherit-global
	Option	Description		
	<i>inherit-global</i>	Control automatic IP address assignment status using the central FortiIPAM config.		
	<i>enable</i>	Enable automatic IP address assignment of this interface by FortiIPAM.		
	<i>disable</i>	Disable automatic IP address assignment of this interface by FortiIPAM.		
ipmac	Enable/disable IP/MAC binding.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IP/MAC binding.		
	<i>disable</i>	Disable IP/MAC binding.		
ips-sniffer-mode	Enable/disable the use of this interface as a one-armed sniffer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPS sniffer mode.		
	<i>disable</i>	Disable IPS sniffer mode.		

Parameter	Description	Type	Size	Default
ipunnumbered	Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.	ipv4-address	Not Specified	0.0.0.0
l2forward	Enable/disable L2 forwarding.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable L2 forwarding.		
	<i>disable</i>	Disable L2 forwarding.		
l2tp-client *	Enable/disable this interface as a Layer 2 Tunnelling Protocol (L2TP) client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable L2TP client.		
	<i>disable</i>	Disable L2TP client.		
lACP-ha-secondary	LACP HA secondary member.	option	-	enable
	Option	Description		
	<i>enable</i>	Allow HA secondary member to send/receive LACP messages.		
	<i>disable</i>	Block HA secondary member from sending/receiving LACP messages.		
lACP-mode	LACP mode.	option	-	active
	Option	Description		
	<i>static</i>	Use static aggregation, do not send and ignore any LACP messages.		
	<i>passive</i>	Passively use LACP to negotiate 802.3ad aggregation.		
	<i>active</i>	Actively use LACP to negotiate 802.3ad aggregation.		
lACP-speed	How often the interface sends LACP messages.	option	-	slow
	Option	Description		
	<i>slow</i>	Send LACP message every 30 seconds.		
	<i>fast</i>	Send LACP message every second.		

Parameter	Description	Type	Size	Default								
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5								
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3								
link-up-delay	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000	50								
lldp-network-policy	LLDP-MED network policy profile.	string	Maximum length: 35									
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reception of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td>disable</td><td>Disable reception of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td>vdom</td><td>Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.</td></tr></table>				Option	Description	enable	Enable reception of Link Layer Discovery Protocol (LLDP).	disable	Disable reception of Link Layer Discovery Protocol (LLDP).	vdom	Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.
Option	Description											
enable	Enable reception of Link Layer Discovery Protocol (LLDP).											
disable	Disable reception of Link Layer Discovery Protocol (LLDP).											
vdom	Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.											
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable transmission of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td>disable</td><td>Disable transmission of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td>vdom</td><td>Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.</td></tr></table>				Option	Description	enable	Enable transmission of Link Layer Discovery Protocol (LLDP).	disable	Disable transmission of Link Layer Discovery Protocol (LLDP).	vdom	Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.
Option	Description											
enable	Enable transmission of Link Layer Discovery Protocol (LLDP).											
disable	Disable transmission of Link Layer Discovery Protocol (LLDP).											
vdom	Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.											
macaddr	Change the interface's MAC address.	mac-address	Not Specified	00:00:00:00:00:00**								
managed-subnetwork-size	Number of IP addresses to be allocated by FortiPAM and used by this FortiGate unit's DHCP server settings.	option	-	256								

Parameter	Description	Type	Size	Default
	Option	Description		
	4	Allocate a subnet with 4 IP addresses.		
	8	Allocate a subnet with 8 IP addresses.		
	16	Allocate a subnet with 16 IP addresses.		
	32	Allocate a subnet with 32 IP addresses.		
	64	Allocate a subnet with 64 IP addresses.		
	128	Allocate a subnet with 128 IP addresses.		
	256	Allocate a subnet with 256 IP addresses.		
	512	Allocate a subnet with 512 IP addresses.		
	1024	Allocate a subnet with 1024 IP addresses.		
	2048	Allocate a subnet with 2048 IP addresses.		
	4096	Allocate a subnet with 4096 IP addresses.		
	8192	Allocate a subnet with 8192 IP addresses.		
	16384	Allocate a subnet with 16384 IP addresses.		
	32768	Allocate a subnet with 32768 IP addresses.		
	65536	Allocate a subnet with 65536 IP addresses.		
	131072	Allocate a subnet with 131072 IP addresses.		
	262144	Allocate a subnet with 262144 IP addresses.		
	524288	Allocate a subnet with 524288 IP addresses.		
	1048576	Allocate a subnet with 1048576 IP addresses.		
	2097152	Allocate a subnet with 2097152 IP addresses.		
	4194304	Allocate a subnet with 4194304 IP addresses.		
	8388608	Allocate a subnet with 8388608 IP addresses.		
16777216	Allocate a subnet with 16777216 IP addresses.			
management-ip	High Availability in-band management IP address of this interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
measured-downstream-bandwidth	Measured downstream bandwidth (kbps).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default								
measured-upstream-bandwidth	Measured upstream bandwidth (kbps).	integer	Minimum value: 0 0 Maximum value: 4294967295									
mediatype *	Select SFP media interface type	option	-	serdes-sfp **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>serdes-sfp</i></td><td>SFP using SerDes Media Interface</td></tr><tr><td><i>sgmii-sfp</i></td><td>SFP using SGMII Media Interface</td></tr><tr><td><i>serdes-copper-sfp</i></td><td>Copper SFP using SerDes media Interface.</td></tr></table>	Option	Description	<i>serdes-sfp</i>	SFP using SerDes Media Interface	<i>sgmii-sfp</i>	SFP using SGMII Media Interface	<i>serdes-copper-sfp</i>	Copper SFP using SerDes media Interface.			
Option	Description											
<i>serdes-sfp</i>	SFP using SerDes Media Interface											
<i>sgmii-sfp</i>	SFP using SGMII Media Interface											
<i>serdes-copper-sfp</i>	Copper SFP using SerDes media Interface.											
member <interface-name>	Physical interfaces that belong to the aggregate or redundant interface. Physical interface name.	string	Maximum length: 79									
min-links	Minimum number of aggregated ports that must be up.	integer	Minimum value: 1 1 Maximum value: 32									
min-links-down	Action to take when less than the configured minimum number of links are active.	option	-	operational								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>operational</i></td><td>Set the aggregate operationally down.</td></tr><tr><td><i>administrative</i></td><td>Set the aggregate administratively down.</td></tr></table>	Option	Description	<i>operational</i>	Set the aggregate operationally down.	<i>administrative</i>	Set the aggregate administratively down.					
Option	Description											
<i>operational</i>	Set the aggregate operationally down.											
<i>administrative</i>	Set the aggregate administratively down.											
mirroring-direction *	Port mirroring direction.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rx</i></td><td>Port mirroring receive direction only.</td></tr><tr><td><i>tx</i></td><td>Port mirroring transmit direction only.</td></tr><tr><td><i>both</i></td><td>Port mirroring both directions.</td></tr></table>	Option	Description	<i>rx</i>	Port mirroring receive direction only.	<i>tx</i>	Port mirroring transmit direction only.	<i>both</i>	Port mirroring both directions.			
Option	Description											
<i>rx</i>	Port mirroring receive direction only.											
<i>tx</i>	Port mirroring transmit direction only.											
<i>both</i>	Port mirroring both directions.											
mirroring-port *	Mirroring port.	string	Maximum length: 15									
mode	Addressing mode (static, DHCP, PPPoE).	option	-	static								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>static</i>	Static setting.		
	<i>dhcp</i>	External DHCP client mode.		
	<i>pppoe</i>	External PPPoE mode.		
monitor-bandwidth	Enable monitoring bandwidth on this interface.	option	-	disable
	Option Description			
	<i>enable</i>	Enable monitoring bandwidth on this interface.		
	<i>disable</i>	Disable monitoring bandwidth on this interface.		
mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295	1500
mtu-override	Enable to set a custom MTU for this interface.	option	-	disable
	Option Description			
	<i>enable</i>	Override default MTU.		
	<i>disable</i>	Use default MTU.		
mux-type *	Multiplexer type.	option	-	llc-encaps
	Option Description			
	<i>llc-encaps</i>	LLC encapsulation.		
	<i>vc-encaps</i>	VC encapsulation.		
name	Name.	string	Maximum length: 15	
ndiscforward	Enable/disable NDISC forwarding.	option	-	enable
	Option Description			
	<i>enable</i>	Enable NDISC forwarding.		
	<i>disable</i>	Disable NDISC forwarding.		
netbios-forward	Enable/disable NETBIOS forwarding.	option	-	disable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NETBIOS forwarding.</td></tr><tr><td><i>enable</i></td><td>Enable NETBIOS forwarding.</td></tr></table>	Option	Description	<i>disable</i>	Disable NETBIOS forwarding.	<i>enable</i>	Enable NETBIOS forwarding.							
	Option	Description												
	<i>disable</i>	Disable NETBIOS forwarding.												
<i>enable</i>	Enable NETBIOS forwarding.													
netflow-sample-rate	NetFlow sample rate. Sample one packet every configured number of packets (1 - 65535, default = 1, which means standard NetFlow where all packets are sampled).	integer	Minimum value: 1 1 Maximum value: 65535											
netflow-sampler	Enable/disable NetFlow on this interface and set the data that NetFlow collects (rx, tx, or both).	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NetFlow protocol on this interface.</td></tr><tr><td><i>tx</i></td><td>Monitor transmitted traffic on this interface.</td></tr><tr><td><i>rx</i></td><td>Monitor received traffic on this interface.</td></tr><tr><td><i>both</i></td><td>Monitor transmitted/received traffic on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable NetFlow protocol on this interface.	<i>tx</i>	Monitor transmitted traffic on this interface.	<i>rx</i>	Monitor received traffic on this interface.	<i>both</i>	Monitor transmitted/received traffic on this interface.			
	Option	Description												
	<i>disable</i>	Disable NetFlow protocol on this interface.												
	<i>tx</i>	Monitor transmitted traffic on this interface.												
	<i>rx</i>	Monitor received traffic on this interface.												
<i>both</i>	Monitor transmitted/received traffic on this interface.													
netflow-sampler-id	Netflow sampler ID.	integer	Minimum value: 0 1 Maximum value: 254											
np-qos-profile *	NP QoS profile ID.	integer	Minimum value: 0 0 Maximum value: 15											
outbandwidth	Bandwidth limit for outgoing traffic (0 - 80000000 kbps).	integer	Minimum value: 0 0 Maximum value: 80000000 **											
padt-retry-timeout	PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time.	integer	Minimum value: 1 0 Maximum value: 4294967295											
password	PPPoE account's password.	password	Not Specified											
phy-mode *	DSL physical mode.	option	-	vdsl										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vdsl</i></td><td>VDSL.</td></tr></table>	Option	Description	<i>vdsl</i>	VDSL.									
	Option	Description												
<i>vdsl</i>	VDSL.													

Parameter	Description	Type	Size	Default																		
ping-serv-status	PING server status. Read-only.	integer	Minimum value: 0 0 Maximum value: 255																			
poe *	Enable/disable PoE status.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable PoE status.</td></tr><tr><td>disable</td><td>Disable PoE status.</td></tr></table>	Option	Description	enable	Enable PoE status.	disable	Disable PoE status.															
Option	Description																					
enable	Enable PoE status.																					
disable	Disable PoE status.																					
polling-interval	sFlow polling interval in seconds (1 - 255).	integer	Minimum value: 20 1 Maximum value: 255																			
port-mirroring *	Enable/disable NP port mirroring.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NP port mirroring.</td></tr><tr><td>enable</td><td>Enable NP port mirroring.</td></tr></table>	Option	Description	disable	Disable NP port mirroring.	enable	Enable NP port mirroring.															
Option	Description																					
disable	Disable NP port mirroring.																					
enable	Enable NP port mirroring.																					
pppoe-egress-cos	CoS in VLAN tag for outgoing PPPoE/PPP packets.	option	-	cos0																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cos0</td><td>CoS 0.</td></tr><tr><td>cos1</td><td>CoS 1.</td></tr><tr><td>cos2</td><td>CoS 2.</td></tr><tr><td>cos3</td><td>CoS 3.</td></tr><tr><td>cos4</td><td>CoS 4.</td></tr><tr><td>cos5</td><td>CoS 5.</td></tr><tr><td>cos6</td><td>CoS 6.</td></tr><tr><td>cos7</td><td>CoS 7.</td></tr></table>	Option	Description	cos0	CoS 0.	cos1	CoS 1.	cos2	CoS 2.	cos3	CoS 3.	cos4	CoS 4.	cos5	CoS 5.	cos6	CoS 6.	cos7	CoS 7.			
Option	Description																					
cos0	CoS 0.																					
cos1	CoS 1.																					
cos2	CoS 2.																					
cos3	CoS 3.																					
cos4	CoS 4.																					
cos5	CoS 5.																					
cos6	CoS 6.																					
cos7	CoS 7.																					
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IP address negotiating for unnumbered.</td></tr><tr><td>disable</td><td>Disable IP address negotiating for unnumbered.</td></tr></table>	Option	Description	enable	Enable IP address negotiating for unnumbered.	disable	Disable IP address negotiating for unnumbered.															
Option	Description																					
enable	Enable IP address negotiating for unnumbered.																					
disable	Disable IP address negotiating for unnumbered.																					

Parameter	Description	Type	Size	Default
pptp-auth-type	PPTP authentication type.	option	-	auto
	Option Description			
	<i>auto</i>	Automatically choose authentication.		
	<i>pap</i>	PAP authentication.		
	<i>chap</i>	CHAP authentication.		
	<i>mschapv1</i>	MS-CHAPv1 authentication.		
	<i>mschapv2</i>	MS-CHAPv2 authentication.		
pptp-client	Enable/disable PPTP client.	option	-	disable
	Option Description			
	<i>enable</i>	Enable PPTP client.		
	<i>disable</i>	Disable PPTP client.		
pptp-password	PPTP password.	password	Not Specified	
pptp-server-ip	PPTP server IP address.	ipv4-address	Not Specified	0.0.0.0
pptp-timeout	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535	0
pptp-user	PPTP user name.	string	Maximum length: 64	
preserve-session-route	Enable/disable preservation of session route when dirty.	option	-	disable
	Option Description			
	<i>enable</i>	Enable preservation of session route when dirty.		
	<i>disable</i>	Disable preservation of session route when dirty.		
priority	Priority of learned routes.	integer	Minimum value: 1 Maximum value: 65535	1
priority-override	Enable/disable fail back to higher priority port once recovered.	option	-	enable
	Option Description			
	<i>enable</i>	Enable fail back to higher priority port once recovered.		
	<i>disable</i>	Disable fail back to higher priority port once recovered.		

Parameter	Description	Type	Size	Default
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-	disable
	Option	Description		
	enable	Enable proxy captive portal on this interface.		
	disable	Disable proxy captive portal on this interface.		
pvc-atm-qos *	SFP-DSL ADSL Fallback PVC ATM QoS.	option	-	ubr
	Option	Description		
	cbr	ATM QoS CBR.		
	rt-vbr	ATM QoS rt-VBR.		
	nrt-vbr	ATM QoS nrt-VBR.		
	ubr	ATM QoS CCBR.		
pvc-chan *	SFP-DSL ADSL Fallback PVC Channel.	integer	Minimum value: 0 0 Maximum value: 7	
pvc-crc *	SFP-DSL ADSL Fallback PVC CRC Option: bit0: sar LLC preserve, bit1: ream LLC preserve, bit2: ream VC-MUX has crc.	integer	Minimum value: 2 0 Maximum value: 7	
pvc-pcr *	SFP-DSL ADSL Fallback PVC Packet Cell Rate in cells (0 - 5500).	integer	Minimum value: 0 0 Maximum value: 5500	
pvc-scr *	SFP-DSL ADSL Fallback PVC Sustainable Cell Rate in cells (0 - 5500).	integer	Minimum value: 0 0 Maximum value: 5500	
pvc-vlan-id *	SFP-DSL ADSL Fallback PVC VLAN ID.	integer	Minimum value: 7 1 Maximum value: 4094	
pvc-vlan-rx-id *	SFP-DSL ADSL Fallback PVC VLANID RX.	integer	Minimum value: 7 1 Maximum value: 4094	
pvc-vlan-rx-op *	SFP-DSL ADSL Fallback PVC VLAN RX op.	option	-	pass-through

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass-through</i></td><td>PVC VLAN Tag Passthrough.</td></tr><tr><td><i>replace</i></td><td>PVC VLAN Tag Replace.</td></tr><tr><td><i>remove</i></td><td>PVC VLAN Tag Remove.</td></tr></table>	Option	Description	<i>pass-through</i>	PVC VLAN Tag Passthrough.	<i>replace</i>	PVC VLAN Tag Replace.	<i>remove</i>	PVC VLAN Tag Remove.			
	Option	Description										
	<i>pass-through</i>	PVC VLAN Tag Passthrough.										
	<i>replace</i>	PVC VLAN Tag Replace.										
<i>remove</i>	PVC VLAN Tag Remove.											
pvc-vlan-tx-id *	SFP-DSL ADSL Fallback PVC VLAN ID TX.	integer	Minimum value: 7 1 Maximum value: 4094									
pvc-vlan-tx-op *	SFP-DSL ADSL Fallback PVC VLAN TX op.	option	-	remove								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass-through</i></td><td>PVC VLAN Tag Passthrough.</td></tr><tr><td><i>replace</i></td><td>PVC VLAN Tag Replace.</td></tr><tr><td><i>remove</i></td><td>PVC VLAN Tag Remove.</td></tr></table>	Option	Description	<i>pass-through</i>	PVC VLAN Tag Passthrough.	<i>replace</i>	PVC VLAN Tag Replace.	<i>remove</i>	PVC VLAN Tag Remove.			
	Option	Description										
	<i>pass-through</i>	PVC VLAN Tag Passthrough.										
	<i>replace</i>	PVC VLAN Tag Replace.										
<i>remove</i>	PVC VLAN Tag Remove.											
reachable-time	IPv4 reachable time in milliseconds (30000 - 3600000, default = 30000).	integer	Minimum value: 30000 Maximum value: 3600000	30000								
redundant-interface	Redundant interface. Read-only.	string	Maximum length: 15									
remote-ip	Remote IP address of tunnel.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								
replacemsg-override-group	Replacement message override group.	string	Maximum length: 35									
retransmission *	Enable/disable DSL retransmission.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable retransmission.</td></tr><tr><td><i>enable</i></td><td>Enable retransmission.</td></tr></table>	Option	Description	<i>disable</i>	Disable retransmission.	<i>enable</i>	Enable retransmission.					
	Option	Description										
	<i>disable</i>	Disable retransmission.										
<i>enable</i>	Enable retransmission.											
ring-rx *	RX ring size.	integer	Minimum value: 0 0 Maximum value: 4294967295									

Parameter	Description	Type	Size	Default
ring-tx *	TX ring size.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
role	Interface role.	option	-	undefined
	Option	Description		
	lan	Connected to local network of endpoints.		
	wan	Connected to Internet.		
	dmz	Connected to server zone.		
	undefined	Interface has no specific role.		
sample-direction	Data that NetFlow collects (rx, tx, or both).	option	-	both
	Option	Description		
	tx	Monitor transmitted traffic on this interface.		
	rx	Monitor received traffic on this interface.		
	both	Monitor transmitted/received traffic on this interface.		
sample-rate	sFlow sample rate (10 - 99999).	integer	Minimum value: 10 10 Maximum value: 99999	2000
secondary-IP	Enable/disable adding a secondary IP to this interface.	option	-	disable
	Option	Description		
	enable	Enable secondary IP.		
	disable	Disable secondary IP.		
security-8021x-dynamic-vlan-id *	VLAN ID for virtual switch.	integer	Minimum value: 0 0 Maximum value: 4094	0
security-8021x-master *	802.1X master virtual-switch.	string	Maximum length: 15	
security-8021x-member-mode *	802.1X member mode.	option	-	switch

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>switch</i>	This member will use switch 802.1X configuration.		
	<i>disable</i>	This member will disable 802.1X configuration.		
security-8021x-mode *	802.1X mode.	option	-	default
	Option	Description		
	<i>default</i>	802.1X default mode.		
	<i>dynamic-vlan</i>	802.1X dynamic VLAN (master) mode.		
	<i>fallback</i>	802.1X fallback (master) mode.		
	<i>slave</i>	802.1X slave mode.		
security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35	
security-external-logout	URL of external authentication logout server.	string	Maximum length: 127	
security-external-web	URL of external authentication web server.	var-string	Maximum length: 1023	
security-groups <name>	User groups that can authenticate with the captive portal. Names of user groups that can authenticate with the captive portal.	string	Maximum length: 79	
security-ip-auth-bypass	Enable/disable IP authentication bypass.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IP authentication bypass.		
	<i>disable</i>	Disable IP authentication bypass.		
security-mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable
	Option	Description		
	<i>mac-auth-only</i>	Enable MAC authentication bypass without EAP.		
	<i>enable</i>	Enable MAC authentication bypass.		
	<i>disable</i>	Disable MAC authentication bypass.		

Parameter	Description	Type	Size	Default								
security-mode	Turn on captive portal authentication for this interface.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No security option.</td></tr><tr><td><i>captive-portal</i></td><td>Captive portal authentication.</td></tr><tr><td><i>802.1X</i></td><td>802.1X port-based authentication.</td></tr></table>	Option	Description	<i>none</i>	No security option.	<i>captive-portal</i>	Captive portal authentication.	<i>802.1X</i>	802.1X port-based authentication.			
Option	Description											
<i>none</i>	No security option.											
<i>captive-portal</i>	Captive portal authentication.											
<i>802.1X</i>	802.1X port-based authentication.											
security-redirect-url	URL redirection after disclaimer/authentication.	var-string	Maximum length: 1023									
select-profile-30a-35b *	Select VDSL Profile 30a or 35b.	option	-	35B								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>30A</i></td><td>Enable VDSL Profile 30A.</td></tr><tr><td><i>35B</i></td><td>Enable VDSL Profile 35B.</td></tr></table>	Option	Description	<i>30A</i>	Enable VDSL Profile 30A.	<i>35B</i>	Enable VDSL Profile 35B.					
Option	Description											
<i>30A</i>	Enable VDSL Profile 30A.											
<i>35B</i>	Enable VDSL Profile 35B.											
service-name	PPPoE service name.	string	Maximum length: 63									
sflow-sampler	Enable/disable sFlow on this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sFlow protocol on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable sFlow protocol on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable sFlow protocol on this interface.	<i>disable</i>	Disable sFlow protocol on this interface.					
Option	Description											
<i>enable</i>	Enable sFlow protocol on this interface.											
<i>disable</i>	Disable sFlow protocol on this interface.											
sfp-dsl *	Enable/disable SFP DSL.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SFP DSL.</td></tr><tr><td><i>enable</i></td><td>Enable SFP DSL.</td></tr></table>	Option	Description	<i>disable</i>	Disable SFP DSL.	<i>enable</i>	Enable SFP DSL.					
Option	Description											
<i>disable</i>	Disable SFP DSL.											
<i>enable</i>	Enable SFP DSL.											
sfp-dsl-adsl-fallback *	Enable/disable SFP DSL ADSL fallback.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SFP DSL ADSL fallback.</td></tr><tr><td><i>enable</i></td><td>Enable SFP DSL ADSL fallback.</td></tr></table>	Option	Description	<i>disable</i>	Disable SFP DSL ADSL fallback.	<i>enable</i>	Enable SFP DSL ADSL fallback.					
Option	Description											
<i>disable</i>	Disable SFP DSL ADSL fallback.											
<i>enable</i>	Enable SFP DSL ADSL fallback.											

Parameter	Description	Type	Size	Default																				
sfp-dsl-autodetect *	Enable/disable SFP DSL MAC address autodetect.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SFP DSL MAC address autodetect.</td></tr><tr><td>enable</td><td>Enable SFP DSL MAC address autodetect.</td></tr></table>	Option	Description	disable	Disable SFP DSL MAC address autodetect.	enable	Enable SFP DSL MAC address autodetect.																	
Option	Description																							
disable	Disable SFP DSL MAC address autodetect.																							
enable	Enable SFP DSL MAC address autodetect.																							
sfp-dsl-mac *	SFP DSL MAC address.	mac-address	Not Specified	00:00:00:00:00:00																				
snmp-index	Permanent SNMP Index of the interface.	integer	Minimum value: 0 Maximum value: 2147483647																					
speed	Interface speed. The default setting and the options available depend on the interface hardware.	option	-	auto																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Automatically adjust speed.</td></tr><tr><td>10full</td><td>10M full-duplex.</td></tr><tr><td>10half</td><td>10M half-duplex.</td></tr><tr><td>100full</td><td>100M full-duplex.</td></tr><tr><td>100half</td><td>100M half-duplex.</td></tr><tr><td>1000full</td><td>1000M full-duplex.</td></tr><tr><td>1000auto</td><td>1000M auto adjust.</td></tr><tr><td>10000full</td><td>10G full-duplex.</td></tr><tr><td>10000auto</td><td>10G auto.</td></tr></table>	Option	Description	auto	Automatically adjust speed.	10full	10M full-duplex.	10half	10M half-duplex.	100full	100M full-duplex.	100half	100M half-duplex.	1000full	1000M full-duplex.	1000auto	1000M auto adjust.	10000full	10G full-duplex.	10000auto	10G auto.			
Option	Description																							
auto	Automatically adjust speed.																							
10full	10M full-duplex.																							
10half	10M half-duplex.																							
100full	100M full-duplex.																							
100half	100M half-duplex.																							
1000full	1000M full-duplex.																							
1000auto	1000M auto adjust.																							
10000full	10G full-duplex.																							
10000auto	10G auto.																							
spillover-threshold	Egress Spillover threshold (0 - 16776000 kbps), 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000																					
src-check	Enable/disable source IP check.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source IP check.</td></tr><tr><td>disable</td><td>Disable source IP check.</td></tr></table>	Option	Description	enable	Enable source IP check.	disable	Disable source IP check.																	
Option	Description																							
enable	Enable source IP check.																							
disable	Disable source IP check.																							

Parameter	Description	Type	Size	Default								
status	Bring the interface up or shut the interface down.	option	-	up								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>up</i></td><td>Bring the interface up.</td></tr><tr><td><i>down</i></td><td>Shut the interface down.</td></tr></table>	Option	Description	<i>up</i>	Bring the interface up.	<i>down</i>	Shut the interface down.					
Option	Description											
<i>up</i>	Bring the interface up.											
<i>down</i>	Shut the interface down.											
stp *	Enable/disable STP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable STP.</td></tr><tr><td><i>enable</i></td><td>Enable STP.</td></tr></table>	Option	Description	<i>disable</i>	Disable STP.	<i>enable</i>	Enable STP.					
Option	Description											
<i>disable</i>	Disable STP.											
<i>enable</i>	Enable STP.											
stp-edge *	Enable/disable as STP edge port.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable STP edge port.</td></tr><tr><td><i>enable</i></td><td>Enable STP edge port.</td></tr></table>	Option	Description	<i>disable</i>	Disable STP edge port.	<i>enable</i>	Enable STP edge port.					
Option	Description											
<i>disable</i>	Disable STP edge port.											
<i>enable</i>	Enable STP edge port.											
stp-ha-secondary *	Control STP behavior on HA secondary.	option	-	priority-adjust								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable STP negotiation on HA secondary.</td></tr><tr><td><i>enable</i></td><td>Enable STP negotiation on HA secondary.</td></tr><tr><td><i>priority-adjust</i></td><td>Enable STP negotiation on HA secondary and make priority lower than HA primary.</td></tr></table>	Option	Description	<i>disable</i>	Disable STP negotiation on HA secondary.	<i>enable</i>	Enable STP negotiation on HA secondary.	<i>priority-adjust</i>	Enable STP negotiation on HA secondary and make priority lower than HA primary.			
Option	Description											
<i>disable</i>	Disable STP negotiation on HA secondary.											
<i>enable</i>	Enable STP negotiation on HA secondary.											
<i>priority-adjust</i>	Enable STP negotiation on HA secondary and make priority lower than HA primary.											
stpforward	Enable/disable STP forwarding.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable STP forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable STP forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable STP forwarding.	<i>disable</i>	Disable STP forwarding.					
Option	Description											
<i>enable</i>	Enable STP forwarding.											
<i>disable</i>	Disable STP forwarding.											
stpforward-mode	Configure STP forwarding mode.	option	-	rpl-all-ext-id								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rpl-all-ext-id</i></td><td>Replace all extension IDs (root, bridge).</td></tr></table>	Option	Description	<i>rpl-all-ext-id</i>	Replace all extension IDs (root, bridge).							
Option	Description											
<i>rpl-all-ext-id</i>	Replace all extension IDs (root, bridge).											

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rpl-bridge-ext-id</i></td><td>Replace the bridge extension ID only.</td></tr><tr><td><i>rpl-nothing</i></td><td>Replace nothing.</td></tr></table>	Option	Description	<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.	<i>rpl-nothing</i>	Replace nothing.							
	Option	Description												
	<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.												
<i>rpl-nothing</i>	Replace nothing.													
subst	Enable to always send packets from this interface to a destination MAC address.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send packets from this interface.</td></tr><tr><td><i>disable</i></td><td>Do not send packets from this interface.</td></tr></table>	Option	Description	<i>enable</i>	Send packets from this interface.	<i>disable</i>	Do not send packets from this interface.							
	Option	Description												
	<i>enable</i>	Send packets from this interface.												
<i>disable</i>	Do not send packets from this interface.													
substitute-dst-mac	Destination MAC address that all packets are sent to from this interface.	mac-address	Not Specified	00:00:00:00:00:00										
sw-algorithm *	Frame distribution algorithm for switch.	option	-	default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>l2</i></td><td>Use layer 2 address for distribution.</td></tr><tr><td><i>l3</i></td><td>Use layer 3 address for distribution.</td></tr><tr><td><i>eh</i></td><td>Use enhanced hashing for distribution.</td></tr><tr><td><i>default</i></td><td>Use the hashing that the driver selects during initialization for distribution.</td></tr></table>	Option	Description	<i>l2</i>	Use layer 2 address for distribution.	<i>l3</i>	Use layer 3 address for distribution.	<i>eh</i>	Use enhanced hashing for distribution.	<i>default</i>	Use the hashing that the driver selects during initialization for distribution.			
	Option	Description												
	<i>l2</i>	Use layer 2 address for distribution.												
	<i>l3</i>	Use layer 3 address for distribution.												
	<i>eh</i>	Use enhanced hashing for distribution.												
<i>default</i>	Use the hashing that the driver selects during initialization for distribution.													
swc-first-create *	Initial create for switch-controller VLANs. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295											
swc-vlan *	Creation status for switch-controller VLANs. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295											
switch	Contained in switch. Read-only.	string	Maximum length: 15											
switch-controller-access-vlan *	Block FortiSwitch port-to-port traffic.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.		
	<i>disable</i>	Allow normal VLAN traffic.		
switch-controller-arp-inspection *	Enable/disable/Monitor FortiSwitch ARP inspection.	option	-	disable
	Option Description			
	<i>enable</i>	Enable ARP inspection for FortiSwitch devices.		
	<i>disable</i>	Disable ARP inspection for FortiSwitch devices.		
	<i>monitor</i>	Monitor ARP traffic and update DHCP client database with MAC-VLAN-IP.		
switch-controller-dhcp-snooping *	Switch controller DHCP snooping.	option	-	disable
	Option Description			
	<i>enable</i>	Enable DHCP snooping for FortiSwitch devices.		
	<i>disable</i>	Disable DHCP snooping for FortiSwitch devices.		
switch-controller-dhcp-snooping-option82 *	Switch controller DHCP snooping option82.	option	-	disable
	Option Description			
	<i>enable</i>	Enable DHCP snooping insert option82 for FortiSwitch devices.		
	<i>disable</i>	Disable DHCP snooping insert option82 for FortiSwitch devices.		
switch-controller-dhcp-snooping-verify-mac *	Switch controller DHCP snooping verify MAC.	option	-	disable
	Option Description			
	<i>enable</i>	Enable DHCP snooping verify source MAC for FortiSwitch devices.		
	<i>disable</i>	Disable DHCP snooping verify source MAC for FortiSwitch devices.		

Parameter	Description	Type	Size	Default																		
switch-controller-dynamic *	Integrated FortiLink settings for managed FortiSwitch.	string	Maximum length: 35																			
switch-controller-feature *	Interface's purpose when assigning traffic (read only).	option	-	none																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>VLAN for generic purpose.</td></tr><tr><td>default-vlan</td><td>Default VLAN (native) assigned to all switch ports upon discovery.</td></tr><tr><td>quarantine</td><td>VLAN for quarantined traffic.</td></tr><tr><td>rspan</td><td>VLAN for RSPAN/ERSPAN mirrored traffic.</td></tr><tr><td>voice</td><td>VLAN dedicated for voice devices.</td></tr><tr><td>video</td><td>VLAN dedicated for camera devices.</td></tr><tr><td>nac</td><td>VLAN dedicated for NAC onboarding devices.</td></tr><tr><td>nac-segment</td><td>VLAN dedicated for NAC segment devices.</td></tr></table>	Option	Description	none	VLAN for generic purpose.	default-vlan	Default VLAN (native) assigned to all switch ports upon discovery.	quarantine	VLAN for quarantined traffic.	rspan	VLAN for RSPAN/ERSPAN mirrored traffic.	voice	VLAN dedicated for voice devices.	video	VLAN dedicated for camera devices.	nac	VLAN dedicated for NAC onboarding devices.	nac-segment	VLAN dedicated for NAC segment devices.			
Option	Description																					
none	VLAN for generic purpose.																					
default-vlan	Default VLAN (native) assigned to all switch ports upon discovery.																					
quarantine	VLAN for quarantined traffic.																					
rspan	VLAN for RSPAN/ERSPAN mirrored traffic.																					
voice	VLAN dedicated for voice devices.																					
video	VLAN dedicated for camera devices.																					
nac	VLAN dedicated for NAC onboarding devices.																					
nac-segment	VLAN dedicated for NAC segment devices.																					
switch-controller-igmp-snooping *	Switch controller IGMP snooping.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IGMP snooping.</td></tr><tr><td>disable</td><td>Disable IGMP snooping.</td></tr></table>	Option	Description	enable	Enable IGMP snooping.	disable	Disable IGMP snooping.															
Option	Description																					
enable	Enable IGMP snooping.																					
disable	Disable IGMP snooping.																					
switch-controller-igmp-snooping-fast-leave *	Switch controller IGMP snooping fast-leave.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IGMP snooping fast-leave.</td></tr><tr><td>disable</td><td>Disable IGMP snooping fast-leave.</td></tr></table>	Option	Description	enable	Enable IGMP snooping fast-leave.	disable	Disable IGMP snooping fast-leave.															
Option	Description																					
enable	Enable IGMP snooping fast-leave.																					
disable	Disable IGMP snooping fast-leave.																					
switch-controller-igmp-snooping-proxy *	Switch controller IGMP snooping proxy.	option	-	disable																		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable IGMP snooping proxy.		
	<i>disable</i>	Disable IGMP snooping proxy.		
switch-controller-iot-scanning *	Enable/disable managed FortiSwitch IoT scanning.	option	-	disable
	Option Description			
	<i>enable</i>	Enable IoT scanning for managed FortiSwitch devices.		
	<i>disable</i>	Disable IoT scanning for managed FortiSwitch devices.		
switch-controller-learning-limit *	Limit the number of dynamic MAC addresses on this VLAN (1 - 128, 0 = no limit, default).	integer	Minimum value: 0 0 Maximum value: 128	
switch-controller-mgmt-vlan *	VLAN to use for FortiLink management purposes.	integer	Minimum value: 4094 1 Maximum value: 4094	
switch-controller-nac *	Integrated FortiLink settings for managed FortiSwitch.	string	Maximum length: 35	
switch-controller-netflow-collect *	NetFlow collection and processing.	option	-	disable
	Option Description			
	<i>disable</i>	Disable NetFlow collection.		
	<i>enable</i>	Enable NetFlow collection.		
switch-controller-offload *	Enable/disable managed FortiSwitch routing offload.	option	-	disable
	Option Description			
	<i>enable</i>	Enable routing offload to managed FortiSwitch devices.		
	<i>disable</i>	Disable routing offload to managed FortiSwitch devices.		
switch-controller-offload-gw *	Enable/disable managed FortiSwitch routing offload gateway.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable routing offload gateway to managed FortiSwitch devices.		
	<i>disable</i>	Disable routing offload gateway to managed FortiSwitch devices.		
switch-controller-offload-ip *	IP for routing offload on FortiSwitch.	ipv4-address	Not Specified	0.0.0.0
switch-controller-rspan-mode *	Stop Layer2 MAC learning and interception of BPDUs and other packets on this interface.	option	-	disable
	Option Description			
	<i>disable</i>	Disable RSPAN passthrough mode on this VLAN interface.		
	<i>enable</i>	Enable RSPAN passthrough mode on this VLAN interface.		
switch-controller-source-ip *	Source IP address used in FortiLink over L3 connections.	option	-	outbound
	Option Description			
	<i>outbound</i>	Source IP address is that of the outbound interface.		
	<i>fixed</i>	Source IP address is that of the FortiLink interface.		
switch-controller-traffic-policy *	Switch controller traffic policy for the VLAN.	string	Maximum length: 63	
system-id	Define a system ID for the aggregate interface.	mac-address	Not Specified	00:00:00:00:00:00
system-id-type	Method in which system ID is generated.	option	-	auto
	Option Description			
	<i>auto</i>	Use the MAC address of the first member.		
	<i>user</i>	User-defined system ID.		
tc-mode *	DSL transfer mode.	option	-	ptm
	Option Description			
	<i>ptm</i>	Packet transfer mode.		

Parameter	Description	Type	Size	Default
tcp-mss	TCP maximum segment size. 0 means do not change segment size.	integer	Minimum value: 48 Maximum value: 65535	0
telemetry-discover *	Enable/disable automatic registration of unknown FortiTelemetry agents.	option	-	enable
	Option	Description		
	enable	Enable automatic registration of unknown FortiTelemetry agents.		
	disable	Disable automatic registration of unknown FortiTelemetry agents.		
trunk *	Enable/disable VLAN trunk.	option	-	disable
	Option	Description		
	enable	Enable VLAN trunk on this interface.		
	disable	Disable VLAN trunk on this interface.		
trust-ip-1	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
trust-ip-2	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
trust-ip-3	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
trust-ip6-1	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
trust-ip6-2	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
trust-ip6-3	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
type	Interface type.	option	-	vlan
	Option	Description		
	physical	Physical interface.		

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vlan</i></td><td>VLAN interface.</td></tr><tr><td><i>aggregate</i></td><td>Aggregate interface.</td></tr><tr><td><i>redundant</i></td><td>Redundant interface.</td></tr><tr><td><i>tunnel</i></td><td>Tunnel interface.</td></tr><tr><td><i>vdom-link</i></td><td>VDOM link interface.</td></tr><tr><td><i>loopback</i></td><td>Loopback interface.</td></tr><tr><td><i>switch</i></td><td>Software switch interface.</td></tr><tr><td><i>vap-switch</i></td><td>VAP interface.</td></tr><tr><td><i>wl-mesh</i></td><td>WLAN mesh interface.</td></tr><tr><td><i>fext-wan</i></td><td>FortiExtender interface.</td></tr><tr><td><i>vxlan</i></td><td>VXLAN interface.</td></tr><tr><td><i>geneve</i></td><td>GENEVE interface.</td></tr><tr><td><i>hdlc</i></td><td>T1/E1 interface.</td></tr><tr><td><i>switch-vlan</i></td><td>Switch VLAN interface.</td></tr><tr><td><i>emac-vlan</i></td><td>EMAC VLAN interface.</td></tr><tr><td><i>ssl</i></td><td>SSL VPN client interface.</td></tr><tr><td><i>lan-extension</i></td><td>LAN extension interface.</td></tr></table>	Option	Description	<i>vlan</i>	VLAN interface.	<i>aggregate</i>	Aggregate interface.	<i>redundant</i>	Redundant interface.	<i>tunnel</i>	Tunnel interface.	<i>vdom-link</i>	VDOM link interface.	<i>loopback</i>	Loopback interface.	<i>switch</i>	Software switch interface.	<i>vap-switch</i>	VAP interface.	<i>wl-mesh</i>	WLAN mesh interface.	<i>fext-wan</i>	FortiExtender interface.	<i>vxlan</i>	VXLAN interface.	<i>geneve</i>	GENEVE interface.	<i>hdlc</i>	T1/E1 interface.	<i>switch-vlan</i>	Switch VLAN interface.	<i>emac-vlan</i>	EMAC VLAN interface.	<i>ssl</i>	SSL VPN client interface.	<i>lan-extension</i>	LAN extension interface.			
	Option	Description																																						
	<i>vlan</i>	VLAN interface.																																						
	<i>aggregate</i>	Aggregate interface.																																						
	<i>redundant</i>	Redundant interface.																																						
	<i>tunnel</i>	Tunnel interface.																																						
	<i>vdom-link</i>	VDOM link interface.																																						
	<i>loopback</i>	Loopback interface.																																						
	<i>switch</i>	Software switch interface.																																						
	<i>vap-switch</i>	VAP interface.																																						
	<i>wl-mesh</i>	WLAN mesh interface.																																						
	<i>fext-wan</i>	FortiExtender interface.																																						
	<i>vxlan</i>	VXLAN interface.																																						
	<i>geneve</i>	GENEVE interface.																																						
	<i>hdlc</i>	T1/E1 interface.																																						
	<i>switch-vlan</i>	Switch VLAN interface.																																						
	<i>emac-vlan</i>	EMAC VLAN interface.																																						
	<i>ssl</i>	SSL VPN client interface.																																						
<i>lan-extension</i>	LAN extension interface.																																							
username	Username of the PPPoE account, provided by your ISP.	string	Maximum length: 64																																					
vci *	Virtual Channel ID.	integer	Minimum value: 0 Maximum value: 65535	35																																				
vdom	Interface is in this virtual domain (VDOM).	string	Maximum length: 31																																					
vectoring *	Enable/disable DSL vectoring.	option	-	enable																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable vectoring.</td></tr><tr><td><i>enable</i></td><td>Enable vectoring.</td></tr></table>	Option	Description	<i>disable</i>	Disable vectoring.	<i>enable</i>	Enable vectoring.																																	
	Option	Description																																						
	<i>disable</i>	Disable vectoring.																																						
<i>enable</i>	Enable vectoring.																																							
vindex *	Switch control interface VLAN ID. Read-only.	integer	Minimum value: 0 Maximum value: 65535	0																																				

Parameter	Description	Type	Size	Default								
virtual-mac	Change the interface's virtual MAC address.	mac-address	Not Specified	00:00:00:00:00:00								
vlan-id *	Vlan ID.	integer	Minimum value: 1 0 Maximum value: 4095									
vlan-op-mode *	Configure DSL 802.1q mode.	option	-	passthrough								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tag</td><td>802.1q Tagged.</td></tr><tr><td>untag</td><td>802.1q Un-Tagged.</td></tr><tr><td>passthrough</td><td>802.1q Passthrough.</td></tr></table>	Option	Description	tag	802.1q Tagged.	untag	802.1q Un-Tagged.	passthrough	802.1q Passthrough.			
Option	Description											
tag	802.1q Tagged.											
untag	802.1q Un-Tagged.											
passthrough	802.1q Passthrough.											
vlan-protocol	Ethernet protocol of VLAN.	option	-	8021q								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>8021q</td><td>IEEE 802.1Q.</td></tr><tr><td>8021ad</td><td>IEEE 802.1AD.</td></tr></table>	Option	Description	8021q	IEEE 802.1Q.	8021ad	IEEE 802.1AD.					
Option	Description											
8021q	IEEE 802.1Q.											
8021ad	IEEE 802.1AD.											
vlanforward	Enable/disable traffic forwarding between VLANs on this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable traffic forwarding.</td></tr><tr><td>disable</td><td>Disable traffic forwarding.</td></tr></table>	Option	Description	enable	Enable traffic forwarding.	disable	Disable traffic forwarding.					
Option	Description											
enable	Enable traffic forwarding.											
disable	Disable traffic forwarding.											
vlanid	VLAN ID (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094									
vpi *	Virtual Path ID.	integer	Minimum value: 0 Maximum value: 255									
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 511									
vrrp-virtual-mac	Enable/disable use of virtual MAC for VRRP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of virtual MAC for VRRP.</td></tr><tr><td>disable</td><td>Disable use of virtual MAC for VRRP.</td></tr></table>	Option	Description	enable	Enable use of virtual MAC for VRRP.	disable	Disable use of virtual MAC for VRRP.					
Option	Description											
enable	Enable use of virtual MAC for VRRP.											
disable	Disable use of virtual MAC for VRRP.											

Parameter	Description	Type	Size	Default								
wccp	Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WCCP protocol on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable WCCP protocol on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable WCCP protocol on this interface.	<i>disable</i>	Disable WCCP protocol on this interface.					
Option	Description											
<i>enable</i>	Enable WCCP protocol on this interface.											
<i>disable</i>	Disable WCCP protocol on this interface.											
weight	Default weight for static routes (if route has no weight configured).	integer	Minimum value: 0 Maximum value: 255	0								
wifi-5g-threshold *	Minimal signal strength to be considered as a good 5G AP.	string	Maximum length: 7	-78								
wifi-acl *	Access control for MAC addresses in the MAC list.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>deny</i></td><td>Deny.</td></tr></table>	Option	Description	<i>allow</i>	Allow.	<i>deny</i>	Deny.					
Option	Description											
<i>allow</i>	Allow.											
<i>deny</i>	Deny.											
wifi-ap-band *	How to select the AP to connect.	option	-	any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Connect to the best 2G or 5G AP.</td></tr><tr><td><i>5g-preferred</i></td><td>Connect to the 5G AP if a good 5G AP exists.</td></tr><tr><td><i>5g-only</i></td><td>Only connect to the 5G AP.</td></tr></table>	Option	Description	<i>any</i>	Connect to the best 2G or 5G AP.	<i>5g-preferred</i>	Connect to the 5G AP if a good 5G AP exists.	<i>5g-only</i>	Only connect to the 5G AP.			
Option	Description											
<i>any</i>	Connect to the best 2G or 5G AP.											
<i>5g-preferred</i>	Connect to the 5G AP if a good 5G AP exists.											
<i>5g-only</i>	Only connect to the 5G AP.											
wifi-auth *	WiFi authentication.	option	-	PSK								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>PSK</i></td><td>PSK.</td></tr><tr><td><i>radius</i></td><td>RADIUS.</td></tr><tr><td><i>usergroup</i></td><td>User group.</td></tr></table>	Option	Description	<i>PSK</i>	PSK.	<i>radius</i>	RADIUS.	<i>usergroup</i>	User group.			
Option	Description											
<i>PSK</i>	PSK.											
<i>radius</i>	RADIUS.											
<i>usergroup</i>	User group.											
wifi-auto-connect *	Enable/disable WiFi network auto connect.	option	-	enable								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiFi network auto connect.</td></tr><tr><td><i>disable</i></td><td>Disable WiFi network auto connect.</td></tr></table>	Option	Description	<i>enable</i>	Enable WiFi network auto connect.	<i>disable</i>	Disable WiFi network auto connect.			
	Option	Description								
	<i>enable</i>	Enable WiFi network auto connect.								
<i>disable</i>	Disable WiFi network auto connect.									
wifi-auto-save *	Enable/disable WiFi network automatic save.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiFi network automatic save.</td></tr><tr><td><i>disable</i></td><td>Disable WiFi network automatic save.</td></tr></table>	Option	Description	<i>enable</i>	Enable WiFi network automatic save.	<i>disable</i>	Disable WiFi network automatic save.			
	Option	Description								
	<i>enable</i>	Enable WiFi network automatic save.								
<i>disable</i>	Disable WiFi network automatic save.									
wifi-broadcast-ssid *	Enable/disable SSID broadcast in the beacon.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSID broadcast in the beacon.</td></tr><tr><td><i>disable</i></td><td>Disable SSID broadcast in the beacon.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSID broadcast in the beacon.	<i>disable</i>	Disable SSID broadcast in the beacon.			
	Option	Description								
	<i>enable</i>	Enable SSID broadcast in the beacon.								
<i>disable</i>	Disable SSID broadcast in the beacon.									
wifi-dns-server1 *	DNS server 1.	ipv4-address	Not Specified	0.0.0.0						
wifi-dns-server2 *	DNS server 2.	ipv4-address	Not Specified	0.0.0.0						
wifi-encrypt *	Data encryption.	option	-	AES						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TKIP</i></td><td>TKIP.</td></tr><tr><td><i>AES</i></td><td>AES.</td></tr></table>	Option	Description	<i>TKIP</i>	TKIP.	<i>AES</i>	AES.			
	Option	Description								
	<i>TKIP</i>	TKIP.								
<i>AES</i>	AES.									
wifi-fragment-threshold *	WiFi fragment threshold (800 - 2346).	integer	Minimum value: 800 Maximum value: 2346	2346						
wifi-gateway *	IPv4 default gateway IP address.	ipv4-address	Not Specified	0.0.0.0						
wifi-key *	WiFi WEP Key.	password	Not Specified							
wifi-keyindex *	WEP key index (1 - 4).	integer	Minimum value: 1 Maximum value: 4	1						
wifi-mac-filter *	Enable/disable MAC filter status.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable MAC filter.		
	<i>disable</i>	Disable MAC filter.		
wifi-passphrase *	WiFi pre-shared key for WPA.	password	Not Specified	
wifi-radius-server *	WiFi RADIUS server for WPA.	string	Maximum length: 35	
wifi-rts-threshold *	WiFi RTS threshold (256 - 2346).	integer	Minimum value: 256 Maximum value: 2346	
wifi-security *	Wireless access security of SSID.	option	-	wpa-personal
	Option	Description		
	<i>open</i>	Open.		
	<i>wep64</i>	WEP64.		
	<i>wep128</i>	WEP128.		
	<i>wpa-personal</i>	WPA personal.		
	<i>wpa-enterprise</i>	WPA enterprise.		
	<i>wpa-only-personal</i>	WPA personal only.		
	<i>wpa-only-enterprise</i>	WPA enterprise only.		
	<i>wpa2-only-personal</i>	WPA2 personal only.		
	<i>wpa2-only-enterprise</i>	WPA2 enterprise only.		
wifi-ssid *	IEEE 802.11 Service Set Identifier.	string	Maximum length: 32	fortinet
wifi-usergroup *	WiFi user group for WPA.	string	Maximum length: 35	
wins-ip	WINS server IP.	ipv4-address	Not Specified	0.0.0.0

* This parameter may not exist in some models.

** Values may differ between models.

config client-options

Parameter	Description	Type	Size	Default
code	DHCP client option code.	integer	Minimum value: 0 0 Maximum value: 255	0
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
ip	DHCP option IPs.	user	Not Specified	
type	DHCP client option type.	option	-	hex
		Option	Description	
		hex	DHCP option in hex.	
		string	DHCP option in string.	
		ip	DHCP option in IP.	
		fqdn	DHCP option in domain search option format.	
value	DHCP client option value.	string	Maximum length: 312	

config dhcp-snooping-server-list

Parameter	Description	Type	Size	Default
name	DHCP server name.	string	Maximum length: 35	default
server-ip	IP address for DHCP server.	ipv4-address	Not Specified	0.0.0.0

config egress-queues

Parameter	Description	Type	Size	Default
cos0	CoS profile name for CoS 0.	string	Maximum length: 35	
cos1	CoS profile name for CoS 1.	string	Maximum length: 35	
cos2	CoS profile name for CoS 2.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
cos3	CoS profile name for CoS 3.	string	Maximum length: 35	
cos4	CoS profile name for CoS 4.	string	Maximum length: 35	
cos5	CoS profile name for CoS 5.	string	Maximum length: 35	
cos6	CoS profile name for CoS 6.	string	Maximum length: 35	
cos7	CoS profile name for CoS 7.	string	Maximum length: 35	

config ipv6

Parameter	Description	Type	Size	Default								
autoconf	Enable/disable address auto config.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auto-configuration.</td></tr><tr><td><i>disable</i></td><td>Disable auto-configuration.</td></tr></table>	Option	Description	<i>enable</i>	Enable auto-configuration.	<i>disable</i>	Disable auto-configuration.					
Option	Description											
<i>enable</i>	Enable auto-configuration.											
<i>disable</i>	Disable auto-configuration.											
cli-conn6-status	CLI IPv6 connection status. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295									
dhcp6-client-options	DHCPv6 client options. Read-only.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rapid</i></td><td>Send rapid commit option.</td></tr><tr><td><i>iapd</i></td><td>Send including IA-PD option.</td></tr><tr><td><i>iana</i></td><td>Send including IA-NA option.</td></tr></table>	Option	Description	<i>rapid</i>	Send rapid commit option.	<i>iapd</i>	Send including IA-PD option.	<i>iana</i>	Send including IA-NA option.			
Option	Description											
<i>rapid</i>	Send rapid commit option.											
<i>iapd</i>	Send including IA-PD option.											
<i>iana</i>	Send including IA-NA option.											
dhcp6-information-request	Enable/disable DHCPv6 information request.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCPv6 information request.</td></tr><tr><td><i>disable</i></td><td>Disable DHCPv6 information request.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCPv6 information request.	<i>disable</i>	Disable DHCPv6 information request.					
Option	Description											
<i>enable</i>	Enable DHCPv6 information request.											
<i>disable</i>	Disable DHCPv6 information request.											

Parameter	Description	Type	Size	Default						
dhcp6-prefix-delegation	Enable/disable DHCPv6 prefix delegation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCPv6 prefix delegation.</td></tr><tr><td><i>disable</i></td><td>Disable DHCPv6 prefix delegation.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCPv6 prefix delegation.	<i>disable</i>	Disable DHCPv6 prefix delegation.			
Option	Description									
<i>enable</i>	Enable DHCPv6 prefix delegation.									
<i>disable</i>	Disable DHCPv6 prefix delegation.									
dhcp6-relay-interface-id	DHCP6 relay interface ID.	string	Maximum length: 64							
dhcp6-relay-ip	DHCPv6 relay IP address.	user	Not Specified							
dhcp6-relay-service	Enable/disable DHCPv6 relay.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable DHCPv6 relay</td></tr><tr><td><i>enable</i></td><td>Enable DHCPv6 relay.</td></tr></table>	Option	Description	<i>disable</i>	Disable DHCPv6 relay	<i>enable</i>	Enable DHCPv6 relay.			
Option	Description									
<i>disable</i>	Disable DHCPv6 relay									
<i>enable</i>	Enable DHCPv6 relay.									
dhcp6-relay-source-interface	Enable/disable use of address on this interface as the source address of the relay message.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Use address of the egress interface as source address of the relay message.</td></tr><tr><td><i>enable</i></td><td>Use address of this interface as source address of the relay message.</td></tr></table>	Option	Description	<i>disable</i>	Use address of the egress interface as source address of the relay message.	<i>enable</i>	Use address of this interface as source address of the relay message.			
Option	Description									
<i>disable</i>	Use address of the egress interface as source address of the relay message.									
<i>enable</i>	Use address of this interface as source address of the relay message.									
dhcp6-relay-source-ip	IPv6 address used by the DHCP6 relay as its source IP.	ipv6-address	Not Specified	::						
dhcp6-relay-type	DHCPv6 relay type.	option	-	regular						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>Regular DHCP relay.</td></tr></table>	Option	Description	<i>regular</i>	Regular DHCP relay.					
Option	Description									
<i>regular</i>	Regular DHCP relay.									
icmp6-send-redirect	Enable/disable sending of ICMPv6 redirects.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of ICMPv6 redirects.</td></tr><tr><td><i>disable</i></td><td>Disable sending of ICMPv6 redirects.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of ICMPv6 redirects.	<i>disable</i>	Disable sending of ICMPv6 redirects.			
Option	Description									
<i>enable</i>	Enable sending of ICMPv6 redirects.									
<i>disable</i>	Disable sending of ICMPv6 redirects.									

Parameter	Description	Type	Size	Default																		
interface-identifier	IPv6 interface identifier.	ipv6-address	Not Specified	::																		
ip6-address	Primary IPv6 address prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx.	ipv6-prefix	Not Specified	::/0																		
ip6-adv-rio	Enable/disable sending advertisements with route information option.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending advertisements with route information option.</td></tr><tr><td>disable</td><td>Disable sending advertisements with route information option.</td></tr></table>	Option	Description	enable	Enable sending advertisements with route information option.	disable	Disable sending advertisements with route information option.															
Option	Description																					
enable	Enable sending advertisements with route information option.																					
disable	Disable sending advertisements with route information option.																					
ip6-allowaccess	Allow management access to the interface.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING access.</td></tr><tr><td>https</td><td>HTTPS access.</td></tr><tr><td>ssh</td><td>SSH access.</td></tr><tr><td>snmp</td><td>SNMP access.</td></tr><tr><td>http</td><td>HTTP access.</td></tr><tr><td>telnet</td><td>TELNET access.</td></tr><tr><td>fgfm</td><td>FortiManager access.</td></tr><tr><td>fabric</td><td>Fabric access.</td></tr></table>	Option	Description	ping	PING access.	https	HTTPS access.	ssh	SSH access.	snmp	SNMP access.	http	HTTP access.	telnet	TELNET access.	fgfm	FortiManager access.	fabric	Fabric access.			
Option	Description																					
ping	PING access.																					
https	HTTPS access.																					
ssh	SSH access.																					
snmp	SNMP access.																					
http	HTTP access.																					
telnet	TELNET access.																					
fgfm	FortiManager access.																					
fabric	Fabric access.																					
ip6-default-life	Default life (sec).	integer	Minimum value: 0 Maximum value: 9000	1800																		
ip6-delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0																		
ip6-dns-server-override	Enable/disable using the DNS server acquired by DHCP.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable using the DNS server acquired by DHCP.</td></tr><tr><td>disable</td><td>Disable using the DNS server acquired by DHCP.</td></tr></table>	Option	Description	enable	Enable using the DNS server acquired by DHCP.	disable	Disable using the DNS server acquired by DHCP.															
Option	Description																					
enable	Enable using the DNS server acquired by DHCP.																					
disable	Disable using the DNS server acquired by DHCP.																					

Parameter	Description	Type	Size	Default										
ip6-hop-limit	Hop limit (0 means unspecified).	integer	Minimum value: 0 Maximum value: 255	0										
ip6-link-mtu	IPv6 link MTU.	integer	Minimum value: 1280 Maximum value: 16000	0										
ip6-manage-flag	Enable/disable the managed flag.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the managed IPv6 flag.</td></tr><tr><td><i>disable</i></td><td>Disable the managed IPv6 flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the managed IPv6 flag.	<i>disable</i>	Disable the managed IPv6 flag.							
Option	Description													
<i>enable</i>	Enable the managed IPv6 flag.													
<i>disable</i>	Disable the managed IPv6 flag.													
ip6-max-interval	IPv6 maximum interval (4 to 1800 sec).	integer	Minimum value: 4 Maximum value: 1800	600										
ip6-min-interval	IPv6 minimum interval (3 to 1350 sec).	integer	Minimum value: 3 Maximum value: 1350	198										
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-	static										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Static setting.</td></tr><tr><td><i>dhcp</i></td><td>DHCPv6 client mode.</td></tr><tr><td><i>pppoe</i></td><td>IPv6 over PPPoE mode.</td></tr><tr><td><i>delegated</i></td><td>IPv6 address with delegated prefix.</td></tr></table>	Option	Description	<i>static</i>	Static setting.	<i>dhcp</i>	DHCPv6 client mode.	<i>pppoe</i>	IPv6 over PPPoE mode.	<i>delegated</i>	IPv6 address with delegated prefix.			
Option	Description													
<i>static</i>	Static setting.													
<i>dhcp</i>	DHCPv6 client mode.													
<i>pppoe</i>	IPv6 over PPPoE mode.													
<i>delegated</i>	IPv6 address with delegated prefix.													
ip6-other-flag	Enable/disable the other IPv6 flag.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the other IPv6 flag.</td></tr><tr><td><i>disable</i></td><td>Disable the other IPv6 flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the other IPv6 flag.	<i>disable</i>	Disable the other IPv6 flag.							
Option	Description													
<i>enable</i>	Enable the other IPv6 flag.													
<i>disable</i>	Disable the other IPv6 flag.													
ip6-prefix-mode	Assigning a prefix from DHCP or RA.	option	-	dhcp6										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dhcp6</i></td><td>Use delegated prefix from a DHCPv6 client to form a delegated IPv6 address.</td></tr><tr><td><i>ra</i></td><td>Use prefix from RA to form a delegated IPv6 address.</td></tr></table>	Option	Description	<i>dhcp6</i>	Use delegated prefix from a DHCPv6 client to form a delegated IPv6 address.	<i>ra</i>	Use prefix from RA to form a delegated IPv6 address.							
Option	Description													
<i>dhcp6</i>	Use delegated prefix from a DHCPv6 client to form a delegated IPv6 address.													
<i>ra</i>	Use prefix from RA to form a delegated IPv6 address.													

Parameter	Description	Type	Size	Default								
ip6-reachable-time	IPv6 reachable time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 3600000	0								
ip6-retrans-time	IPv6 retransmit time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 4294967295	0								
ip6-route-pref	Set route preference to the interface (default = medium).	option	-	medium								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>medium</i></td><td>Medium route preferences in RA packet.</td></tr><tr><td><i>high</i></td><td>High route preferences in RA packet.</td></tr><tr><td><i>low</i></td><td>Low route preferences in RA packet.</td></tr></table>				Option	Description	<i>medium</i>	Medium route preferences in RA packet.	<i>high</i>	High route preferences in RA packet.	<i>low</i>	Low route preferences in RA packet.
	Option	Description										
	<i>medium</i>	Medium route preferences in RA packet.										
	<i>high</i>	High route preferences in RA packet.										
<i>low</i>	Low route preferences in RA packet.											
ip6-send-adv	Enable/disable sending advertisements about the interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending advertisements about this interface.</td></tr><tr><td><i>disable</i></td><td>Disable sending advertisements about this interface.</td></tr></table>				Option	Description	<i>enable</i>	Enable sending advertisements about this interface.	<i>disable</i>	Disable sending advertisements about this interface.		
	Option	Description										
	<i>enable</i>	Enable sending advertisements about this interface.										
<i>disable</i>	Disable sending advertisements about this interface.											
ip6-subnet	Subnet to routing prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx.	ipv6-prefix	Not Specified	::/0								
ip6-upstream-interface	Interface name providing delegated information.	string	Maximum length: 15									
nd-cert	Neighbor discovery certificate.	string	Maximum length: 35									
nd-cga-modifier	Neighbor discovery CGA modifier.	user	Not Specified									
nd-mode	Neighbor discovery mode.	option	-	basic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>basic</i></td><td>Do not support SEND.</td></tr><tr><td><i>SEND-compatible</i></td><td>Support SEND.</td></tr></table>				Option	Description	<i>basic</i>	Do not support SEND.	<i>SEND-compatible</i>	Support SEND.		
	Option	Description										
	<i>basic</i>	Do not support SEND.										
<i>SEND-compatible</i>	Support SEND.											

Parameter	Description	Type	Size	Default
nd-security-level	Neighbor discovery security level (0 - 7; 0 = least secure, default = 0).	integer	Minimum value: 0 Maximum value: 7	0
nd-timestamp-delta	Neighbor discovery timestamp delta value (1 - 3600 sec; default = 300).	integer	Minimum value: 1 Maximum value: 3600	300
nd-timestamp-fuzz	Neighbor discovery timestamp fuzz factor (1 - 60 sec; default = 1).	integer	Minimum value: 1 Maximum value: 60	1
ra-send-mtu	Enable/disable sending link MTU in RA packet.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sending link MTU in RA packet.		
	<i>disable</i>	Disable sending link MTU in RA packet.		
unique-autoconf-addr	Enable/disable unique auto config address.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable unique auto-configuration address.		
	<i>disable</i>	Disable unique auto-configuration address.		
vrip6_link_local	Link-local IPv6 address of virtual router.	ipv6-address	Not Specified	::
vrrp-virtual-mac6	Enable/disable virtual MAC for VRRP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable virtual MAC for VRRP.		
	<i>disable</i>	Disable virtual MAC for VRRP.		

config client-options

Parameter	Description	Type	Size	Default
code	DHCPv6 option code.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default										
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0										
ip6	DHCP option IP6s.	user	Not Specified											
type	DHCPv6 option type.	option	-	hex										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hex</td><td>DHCPv6 option in hex.</td></tr><tr><td>string</td><td>DHCPv6 option in string.</td></tr><tr><td>ip6</td><td>DHCPv6 option in IP6.</td></tr><tr><td>fqdn</td><td>DHCPv6 option in domain search option format.</td></tr></table>				Option	Description	hex	DHCPv6 option in hex.	string	DHCPv6 option in string.	ip6	DHCPv6 option in IP6.	fqdn	DHCPv6 option in domain search option format.
	Option	Description												
	hex	DHCPv6 option in hex.												
	string	DHCPv6 option in string.												
	ip6	DHCPv6 option in IP6.												
fqdn	DHCPv6 option in domain search option format.													
value	DHCPv6 option value (hexadecimal value must be even).	string	Maximum length: 312											

config dhcp6-iapd-list

Parameter	Description	Type	Size	Default
iaid	Identity association identifier.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
prefix-hint	DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.	ipv6-network	Not Specified	::/0
prefix-hint-plt	DHCPv6 prefix hint preferred life time (sec), 0 means unlimited lease time.	integer	Minimum value: 0 0 Maximum value: 4294967295	604800
prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 0 Maximum value: 4294967295	2592000

config ip6-delegated-prefix-list

Parameter	Description	Type	Size	Default
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the autonomous flag.		
	<i>disable</i>	Disable the autonomous flag.		
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 0 Maximum value: 4294967295	
onlink-flag	Enable/disable the onlink flag.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the onlink flag.		
	<i>disable</i>	Disable the onlink flag.		
prefix-id	Prefix ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
rdnss	Recursive DNS server option.	user	Not Specified	
rdnss-service	Recursive DNS service option.	option	-	specify
	Option	Description		
	<i>delegated</i>	Delegated RDNSS settings.		
	<i>default</i>	System RDNSS settings.		
	<i>specify</i>	Specify recursive DNS servers.		
subnet	Add subnet ID to routing prefix.	ipv6-network	Not Specified	::/0
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15	

config ip6-dnssl-list

Parameter	Description	Type	Size	Default
dnssl-life-time	DNS search list time in seconds (0 - 4294967295, default = 1800).	integer	Minimum value: 0 0 Maximum value: 4294967295	1800
domain	Domain name.	string	Maximum length: 79	

config ip6-extra-addr

Parameter	Description	Type	Size	Default
prefix	IPv6 address prefix.	ipv6-prefix	Not Specified	::/0

config ip6-prefix-list

Parameter	Description	Type	Size	Default						
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable the autonomous flag.</td></tr><tr><td>disable</td><td>Disable the autonomous flag.</td></tr></table>	Option	Description	enable	Enable the autonomous flag.	disable	Disable the autonomous flag.			
Option	Description									
enable	Enable the autonomous flag.									
disable	Disable the autonomous flag.									
onlink-flag	Enable/disable the onlink flag.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable the onlink flag.</td></tr><tr><td>disable</td><td>Disable the onlink flag.</td></tr></table>	Option	Description	enable	Enable the onlink flag.	disable	Disable the onlink flag.			
Option	Description									
enable	Enable the onlink flag.									
disable	Disable the onlink flag.									
preferred-life-time	Preferred life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	604800						
prefix	IPv6 prefix.	ipv6-network	Not Specified	::/0						
valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000						

config ip6-rdnss-list

Parameter	Description	Type	Size	Default
rdnss	Recursive DNS server option.	ipv6-address	Not Specified	::
rdnss-life-time	Recursive DNS server life time in seconds (0 - 4294967295, default = 1800).	integer	Minimum value: 0 Maximum value: 4294967295	1800

config ip6-route-list

Parameter	Description	Type	Size	Default								
route	IPv6 route.	ipv6-network	Not Specified	::/0								
route-life-time	Route life time in seconds (0 - 65535, default = 1800).	integer	Minimum value: 0 Maximum value: 65535	1800								
route-pref	Set route preference to the interface (default = medium).	option	-	medium								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>medium</td><td>Medium route preferences in RA packet.</td></tr><tr><td>high</td><td>High route preferences in RA packet.</td></tr><tr><td>low</td><td>Low route preferences in RA packet.</td></tr></table>				Option	Description	medium	Medium route preferences in RA packet.	high	High route preferences in RA packet.	low	Low route preferences in RA packet.
Option	Description											
medium	Medium route preferences in RA packet.											
high	High route preferences in RA packet.											
low	Low route preferences in RA packet.											

config vrrp6

Parameter	Description	Type	Size	Default
accept-mode	Enable/disable accept mode.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable accept mode.		
	<i>disable</i>	Disable accept mode.		
adv-interval	Advertisement interval (250 - 255000 milliseconds).	integer	Minimum value: 250 Maximum value: 255000	1000
ignore-default-route	Enable/disable ignoring of default route when checking destination.	option	-	disable
	Option	Description		
	<i>enable</i>	Ignore default route when checking destination.		
	<i>disable</i>	Do not ignore default route when checking destination.		
preempt	Enable/disable preempt mode.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable preempt mode.</td></tr><tr><td><i>disable</i></td><td>Disable preempt mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable preempt mode.	<i>disable</i>	Disable preempt mode.			
	Option	Description								
	<i>enable</i>	Enable preempt mode.								
<i>disable</i>	Disable preempt mode.									
priority	Priority of the virtual router (1 - 255).	integer	Minimum value: 1 Maximum value: 255	100						
start-time	Startup time (1 - 255 seconds).	integer	Minimum value: 1 Maximum value: 255	3						
status	Enable/disable VRRP.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VRRP.</td></tr><tr><td><i>disable</i></td><td>Disable VRRP.</td></tr></table>	Option	Description	<i>enable</i>	Enable VRRP.	<i>disable</i>	Disable VRRP.			
	Option	Description								
	<i>enable</i>	Enable VRRP.								
<i>disable</i>	Disable VRRP.									
vrdst-priority	Priority of the virtual router when the virtual router destination becomes unreachable (0 - 254).	integer	Minimum value: 0 Maximum value: 254	0						
vrdst6	Monitor the route to this destination.	ipv6-address	Not Specified							
vrgrp	VRRP group ID (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	0						
vrid	Virtual router identifier (1 - 255).	integer	Minimum value: 1 Maximum value: 255	0						
vrp6	IPv6 address of the virtual router.	ipv6-address	Not Specified	::						

config l2tp-client-settings

Parameter	Description	Type	Size	Default
auth-type	L2TP authentication type.	option	-	auto

Parameter	Description	Type	Size	Default													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically choose authentication.</td></tr><tr><td><i>pap</i></td><td>PAP authentication.</td></tr><tr><td><i>chap</i></td><td>CHAP authentication.</td></tr><tr><td><i>mschapv1</i></td><td>MS-CHAPv1 authentication.</td></tr><tr><td><i>mschapv2</i></td><td>MS-CHAPv2 authentication.</td></tr></table>		Option	Description	<i>auto</i>	Automatically choose authentication.	<i>pap</i>	PAP authentication.	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.			
	Option	Description															
	<i>auto</i>	Automatically choose authentication.															
	<i>pap</i>	PAP authentication.															
	<i>chap</i>	CHAP authentication.															
	<i>mschapv1</i>	MS-CHAPv1 authentication.															
<i>mschapv2</i>	MS-CHAPv2 authentication.																
defaultgw	Enable/disable default gateway.	option	-	disable													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable default gateway.</td></tr><tr><td><i>disable</i></td><td>Disable default gateway.</td></tr></table>		Option	Description	<i>enable</i>	Enable default gateway.	<i>disable</i>	Disable default gateway.									
	Option	Description															
	<i>enable</i>	Enable default gateway.															
<i>disable</i>	Disable default gateway.																
distance	Distance of learned routes.	integer	Minimum value: 1 Maximum value: 255	2													
hello-interval	L2TP hello message interval in seconds (0 - 3600 sec, default = 60).	integer	Minimum value: 0 Maximum value: 3600	60													
ip	IP. Read-only.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0													
mtu	L2TP MTU.	integer	Minimum value: 40 Maximum value: 65535	1460													
password	L2TP password.	password	Not Specified														
peer-host	L2TP peer host address.	string	Maximum length: 255														
peer-mask	L2TP peer mask.	ipv4-netmask	Not Specified	255.255.255.255													

Parameter	Description	Type	Size	Default
peer-port	L2TP peer port number.	integer	Minimum value: 1 Maximum value: 65535	1701
priority	Priority of learned routes.	integer	Minimum value: 1 Maximum value: 65535	1
user	L2TP user name.	string	Maximum length: 127	

config mirroring-filter

Parameter	Description	Type	Size	Default
filter-dport	Destinatin port of mirroring filter.	integer	Minimum value: 0 Maximum value: 65535	0
filter-dstip	Destinatin IP and mask of mirroring filter.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
filter-protocol	Protocol of mirroring filter.	integer	Minimum value: 0 Maximum value: 255	0
filter-sport	Source port of mirroring filter.	integer	Minimum value: 0 Maximum value: 65535	0
filter-srcip	Source IP and mask of mirroring filter.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0

config secondaryip

Parameter	Description	Type	Size	Default																												
allowaccess	Management access settings for the secondary IP address.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING access.</td></tr><tr><td>https</td><td>HTTPS access.</td></tr><tr><td>ssh</td><td>SSH access.</td></tr><tr><td>snmp</td><td>SNMP access.</td></tr><tr><td>http</td><td>HTTP access.</td></tr><tr><td>telnet</td><td>TELNET access.</td></tr><tr><td>fgfm</td><td>FortiManager access.</td></tr><tr><td>radius-acct</td><td>RADIUS accounting access.</td></tr><tr><td>probe-response</td><td>Probe access.</td></tr><tr><td>fabric</td><td>Security Fabric access.</td></tr><tr><td>ftm</td><td>FTM access.</td></tr><tr><td>speed-test</td><td>Speed test access.</td></tr><tr><td>scim</td><td>System for Cross-domain Identity Management (SCIM) access.</td></tr></table>	Option	Description	ping	PING access.	https	HTTPS access.	ssh	SSH access.	snmp	SNMP access.	http	HTTP access.	telnet	TELNET access.	fgfm	FortiManager access.	radius-acct	RADIUS accounting access.	probe-response	Probe access.	fabric	Security Fabric access.	ftm	FTM access.	speed-test	Speed test access.	scim	System for Cross-domain Identity Management (SCIM) access.			
Option	Description																															
ping	PING access.																															
https	HTTPS access.																															
ssh	SSH access.																															
snmp	SNMP access.																															
http	HTTP access.																															
telnet	TELNET access.																															
fgfm	FortiManager access.																															
radius-acct	RADIUS accounting access.																															
probe-response	Probe access.																															
fabric	Security Fabric access.																															
ftm	FTM access.																															
speed-test	Speed test access.																															
scim	System for Cross-domain Identity Management (SCIM) access.																															
detectprotocol	Protocols used to detect the server.	option	-	ping																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING.</td></tr><tr><td>tcp-echo</td><td>TCP echo.</td></tr><tr><td>udp-echo</td><td>UDP echo.</td></tr></table>	Option	Description	ping	PING.	tcp-echo	TCP echo.	udp-echo	UDP echo.																							
Option	Description																															
ping	PING.																															
tcp-echo	TCP echo.																															
udp-echo	UDP echo.																															
detectserver	Gateway's ping server for this IP.	user	Not Specified																													
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable detect gateway alive for first.</td></tr><tr><td>disable</td><td>Disable detect gateway alive for first.</td></tr></table>	Option	Description	enable	Enable detect gateway alive for first.	disable	Disable detect gateway alive for first.																									
Option	Description																															
enable	Enable detect gateway alive for first.																															
disable	Disable detect gateway alive for first.																															

Parameter	Description	Type	Size	Default
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Secondary IP address of the interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
ping-serv-status	PING server status. Read-only.	integer	Minimum value: 0 Maximum value: 255	0
secip-relay-ip	DHCP relay IP address.	user	Not Specified	

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config vrrp

Parameter	Description	Type	Size	Default						
accept-mode	Enable/disable accept mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable accept mode.</td></tr><tr><td><i>disable</i></td><td>Disable accept mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable accept mode.	<i>disable</i>	Disable accept mode.			
Option	Description									
<i>enable</i>	Enable accept mode.									
<i>disable</i>	Disable accept mode.									
adv-interval	Advertisement interval (250 - 255000 milliseconds).	integer	Minimum value: 250 Maximum value: 255000	1000						

Parameter	Description	Type	Size	Default						
ignore-default-route	Enable/disable ignoring of default route when checking destination.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Ignore default route when checking destination.</td></tr><tr><td><i>disable</i></td><td>Do not ignore default route when checking destination.</td></tr></table>	Option	Description	<i>enable</i>	Ignore default route when checking destination.	<i>disable</i>	Do not ignore default route when checking destination.			
Option	Description									
<i>enable</i>	Ignore default route when checking destination.									
<i>disable</i>	Do not ignore default route when checking destination.									
preempt	Enable/disable preempt mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable preempt mode.</td></tr><tr><td><i>disable</i></td><td>Disable preempt mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable preempt mode.	<i>disable</i>	Disable preempt mode.			
Option	Description									
<i>enable</i>	Enable preempt mode.									
<i>disable</i>	Disable preempt mode.									
priority	Priority of the virtual router (1 - 255).	integer	Minimum value: 1 Maximum value: 255	100						
start-time	Startup time (1 - 255 seconds).	integer	Minimum value: 1 Maximum value: 255	3						
status	Enable/disable this VRRP configuration.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this VRRP configuration.</td></tr><tr><td><i>disable</i></td><td>Disable this VRRP configuration.</td></tr></table>	Option	Description	<i>enable</i>	Enable this VRRP configuration.	<i>disable</i>	Disable this VRRP configuration.			
Option	Description									
<i>enable</i>	Enable this VRRP configuration.									
<i>disable</i>	Disable this VRRP configuration.									
version	VRRP version.	option	-	2						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>2</td><td>VRRP version 2.</td></tr><tr><td>3</td><td>VRRP version 3.</td></tr></table>	Option	Description	2	VRRP version 2.	3	VRRP version 3.			
Option	Description									
2	VRRP version 2.									
3	VRRP version 3.									
vrdst	Monitor the route to this destination.	ipv4-address-any	Not Specified							
vrdst-priority	Priority of the virtual router when the virtual router destination becomes unreachable (0 - 254).	integer	Minimum value: 0 Maximum value: 254	0						

Parameter	Description	Type	Size	Default
vrgrp	VRRP group ID (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	0
vrid	Virtual router identifier (1 - 255).	integer	Minimum value: 1 Maximum value: 255	0
vip	IP address of the virtual router.	ipv4-address-any	Not Specified	0.0.0.0

config proxy-arp

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Set IP addresses of proxy ARP.	user	Not Specified	

config wifi-mac-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00

config wifi-networks

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default										
wifi-ca-certificate	CA certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 79											
wifi-client-certificate	Client certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35											
wifi-eap-type	WPA2/WPA3-ENTERPRISE EAP Method.	option	-	peap										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>both</i></td><td>EAP PEAP and TLS.</td></tr><tr><td><i>tls</i></td><td>EAP TLS.</td></tr><tr><td><i>peap</i></td><td>EAP PEAP.</td></tr></table>	Option	Description	<i>both</i>	EAP PEAP and TLS.	<i>tls</i>	EAP TLS.	<i>peap</i>	EAP PEAP.					
Option	Description													
<i>both</i>	EAP PEAP and TLS.													
<i>tls</i>	EAP TLS.													
<i>peap</i>	EAP PEAP.													
wifi-encrypt	Data encryption.	option	-	AES										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TKIP</i></td><td>TKIP.</td></tr><tr><td><i>AES</i></td><td>AES.</td></tr></table>	Option	Description	<i>TKIP</i>	TKIP.	<i>AES</i>	AES.							
Option	Description													
<i>TKIP</i>	TKIP.													
<i>AES</i>	AES.													
wifi-key	WiFi WEP Key.	password	Not Specified											
wifi-keyindex	WEP key index (1 - 4).	integer	Minimum value: 1 1 Maximum value: 4											
wifi-passphrase	WiFi pre-shared key for WPA-PSK or password for WPA3-SAE and WPA2/WPA3-ENTERPRISE.	password	Not Specified											
wifi-private-key	Private key for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35											
wifi-private-key-password	Password for private key file for WPA2/WPA3-ENTERPRISE.	password	Not Specified											
wifi-security	Wireless access security of SSID.	option	-	wpa-personal										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wep64</i></td><td>WEP64.</td></tr><tr><td><i>wep128</i></td><td>WEP128.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA personal.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>wep64</i>	WEP64.	<i>wep128</i>	WEP128.	<i>wpa-personal</i>	WPA personal.			
Option	Description													
<i>open</i>	Open.													
<i>wep64</i>	WEP64.													
<i>wep128</i>	WEP128.													
<i>wpa-personal</i>	WPA personal.													

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wpa-only-personal</i>	WPA personal only.		
	<i>wpa2-only-personal</i>	WPA2 personal only.		
	<i>wpa3-sae</i>	WPA3 SAE.		
	<i>owe</i>	OWE.		
	<i>wpa-enterprise</i>	WPA2/WPA3 ENTERPRISE.		
wifi-ssid	IEEE 802.11 Service Set Identifier.	string	Maximum length: 32	fortinet
wifi-username	Username for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 64	fortinet

config system ipam

Configure IP address management services.

```

config system ipam
  Description: Configure IP address management services.
  set automatic-conflict-resolution [disable|enable]
  set manage-lan-addresses [disable|enable]
  set manage-lan-extension-addresses [disable|enable]
  set manage-ssid-addresses [disable|enable]
  config pools
    Description: Configure IPAM pools.
    edit <name>
      set description {string}
      config exclude
        Description: Configure pool exclude subnets.
        edit <ID>
          set exclude-subnet {ipv4-classnet}
        next
      end
      set subnet {ipv4-classnet}
    next
  end
  set require-subnet-size-match [disable|enable]
  config rules
    Description: Configure IPAM allocation rules.
    edit <name>
      set description {string}
      set device <name1>, <name2>, ...
      set dhcp [enable|disable]

```

```

        set interface <name1>, <name2>, ...
        set pool <name1>, <name2>, ...
        set role [any|lan|...]
    next
end
set server-type {option}
set status [enable|disable]
end

```

config system ipam

Parameter	Description	Type	Size	Default						
automatic-conflict-resolution	Enable/disable automatic conflict resolution.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable automatic conflict resolution.</td></tr><tr><td>enable</td><td>Enable automatic conflict resolution.</td></tr></table>	Option	Description	disable	Disable automatic conflict resolution.	enable	Enable automatic conflict resolution.			
Option	Description									
disable	Disable automatic conflict resolution.									
enable	Enable automatic conflict resolution.									
manage-lan-addresses	Enable/disable default management of LAN interface addresses.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable LAN interface address management by default.</td></tr><tr><td>enable</td><td>Enable LAN interface address management by default.</td></tr></table>	Option	Description	disable	Disable LAN interface address management by default.	enable	Enable LAN interface address management by default.			
Option	Description									
disable	Disable LAN interface address management by default.									
enable	Enable LAN interface address management by default.									
manage-lan-extension-addresses	Enable/disable default management of FortiExtender LAN extension interface addresses.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable FortiExtender LAN extension interface address management by default.</td></tr><tr><td>enable</td><td>Enable FortiExtender LAN extension interface address management by default.</td></tr></table>	Option	Description	disable	Disable FortiExtender LAN extension interface address management by default.	enable	Enable FortiExtender LAN extension interface address management by default.			
Option	Description									
disable	Disable FortiExtender LAN extension interface address management by default.									
enable	Enable FortiExtender LAN extension interface address management by default.									
manage-ssid-addresses	Enable/disable default management of FortiAP SSID addresses.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable FortiAP SSID address management by default.</td></tr><tr><td>enable</td><td>Enable FortiAP SSID address management by default.</td></tr></table>	Option	Description	disable	Disable FortiAP SSID address management by default.	enable	Enable FortiAP SSID address management by default.			
Option	Description									
disable	Disable FortiAP SSID address management by default.									
enable	Enable FortiAP SSID address management by default.									

Parameter	Description	Type	Size	Default						
require-subnet-size-match	Enable/disable reassignment of subnets to make requested and actual sizes match.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable requiring subnet sizes to match.</td></tr><tr><td>enable</td><td>Enable requiring subnet sizes to match.</td></tr></table>	Option	Description	disable	Disable requiring subnet sizes to match.	enable	Enable requiring subnet sizes to match.			
Option	Description									
disable	Disable requiring subnet sizes to match.									
enable	Enable requiring subnet sizes to match.									
server-type	Configure the type of IPAM server to use.	option	-	fabric-root						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fabric-root</td><td>Use the IPAM server running on the Security Fabric root.</td></tr></table>	Option	Description	fabric-root	Use the IPAM server running on the Security Fabric root.					
Option	Description									
fabric-root	Use the IPAM server running on the Security Fabric root.									
status	Enable/disable IP address management services.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable integration with IP address management services.</td></tr><tr><td>disable</td><td>Disable integration with IP address management services.</td></tr></table>	Option	Description	enable	Enable integration with IP address management services.	disable	Disable integration with IP address management services.			
Option	Description									
enable	Enable integration with IP address management services.									
disable	Disable integration with IP address management services.									

config pools

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
name	IPAM pool name.	string	Maximum length: 79	
subnet	Configure IPAM pool subnet, Class A - Class B subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config exclude

Parameter	Description	Type	Size	Default
ID	Exclude ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
exclude-subnet	Configure subnet to exclude from the IPAM pool.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config rules

Parameter	Description	Type	Size	Default												
description	Description.	string	Maximum length: 127													
device <name>	Configure serial number or wildcard of FortiGate to match. FortiGate serial number or wildcard.	string	Maximum length: 79													
dhcp	Enable/disable DHCP server for matching IPAM interfaces.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DHCP server on matched IPAM interface.</td></tr><tr><td>disable</td><td>Disable DHCP server on matched IPAM interface.</td></tr></table>	Option	Description	enable	Enable DHCP server on matched IPAM interface.	disable	Disable DHCP server on matched IPAM interface.									
Option	Description															
enable	Enable DHCP server on matched IPAM interface.															
disable	Disable DHCP server on matched IPAM interface.															
interface <name>	Configure name or wildcard of interface to match. Interface name or wildcard.	string	Maximum length: 79													
name	IPAM rule name.	string	Maximum length: 79													
pool <name>	Configure name of IPAM pool to use. IPAM pool name.	string	Maximum length: 79													
role	Configure role of interface to match.	option	-	any												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>any</td><td>Match any interface role.</td></tr><tr><td>lan</td><td>Match interface role lan.</td></tr><tr><td>wan</td><td>Match interface role wan.</td></tr><tr><td>dmz</td><td>Match interface role dmz.</td></tr><tr><td>undefined</td><td>Match interface role undefined.</td></tr></table>	Option	Description	any	Match any interface role.	lan	Match interface role lan.	wan	Match interface role wan.	dmz	Match interface role dmz.	undefined	Match interface role undefined.			
Option	Description															
any	Match any interface role.															
lan	Match interface role lan.															
wan	Match interface role wan.															
dmz	Match interface role dmz.															
undefined	Match interface role undefined.															

config system ipip-tunnel

Configure IP in IP Tunneling.

```
config system ipip-tunnel
  Description: Configure IP in IP Tunneling.
  edit <name>
    set auto-asic-offload [enable|disable]
    set interface {string}
    set local-gw {ipv4-address-any}
```

```

        set remote-gw {ipv4-address}
        set use-sdwan [disable|enable]
    next
end

```

config system ipip-tunnel

Parameter	Description	Type	Size	Default						
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auto ASIC offloading.</td></tr><tr><td><i>disable</i></td><td>Disable ASIC offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable auto ASIC offloading.	<i>disable</i>	Disable ASIC offloading.			
Option	Description									
<i>enable</i>	Enable auto ASIC offloading.									
<i>disable</i>	Disable ASIC offloading.									
interface	Interface name that is associated with the incoming traffic from available options.	string	Maximum length: 15							
local-gw	IPv4 address for the local gateway.	ipv4-address-any	Not Specified	0.0.0.0						
name	IPIP Tunnel name.	string	Maximum length: 15							
remote-gw	IPv4 address for the remote gateway.	ipv4-address	Not Specified	0.0.0.0						
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of SD-WAN to reach remote gateway.</td></tr><tr><td><i>enable</i></td><td>Enable use of SD-WAN to reach remote gateway.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of SD-WAN to reach remote gateway.	<i>enable</i>	Enable use of SD-WAN to reach remote gateway.			
Option	Description									
<i>disable</i>	Disable use of SD-WAN to reach remote gateway.									
<i>enable</i>	Enable use of SD-WAN to reach remote gateway.									

* This parameter may not exist in some models.

config system ips

Configure IPS system settings.

```

config system ips
    Description: Configure IPS system settings.
    set override-signature-hold-by-id [enable|disable]
    set signature-hold-time {user}
end

```

config system ips

Parameter	Description	Type	Size	Default
override-signature-hold-by-id	Enable/disable override of hold of triggering signatures that are specified by IDs regardless of hold.	option	-	enable
	Option	Description		
	<i>enable</i>	Allow the signatures specified by IDs to be triggered even if they are on hold.		
	<i>disable</i>	Do not trigger the signatures that are on hold.		
signature-hold-time	Time to hold and monitor IPS signatures. Format <#d##h> (day range: 0 - 21, hour range: 0 - 23, max hold time: 21d0h, default hold time: 0d0h).	user	Not Specified	0h

config system ipsec-aggregate

Configure an aggregate of IPsec tunnels.

```
config system ipsec-aggregate
  Description: Configure an aggregate of IPsec tunnels.
  edit <name>
    set algorithm [L3|L4|...]
    set member <tunnel-name1>, <tunnel-name2>, ...
  next
end
```

config system ipsec-aggregate

Parameter	Description	Type	Size	Default
algorithm	Frame distribution algorithm.	option	-	round-robin
	Option	Description		
	L3	Use layer 3 address for distribution.		
	L4	Use layer 4 information for distribution.		
	round-robin	Per-packet round-robin distribution.		
	redundant	Use first tunnel that is up for all traffic.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>weighted-round-robin</i>	Weighted round-robin distribution.		
member <tunnel-name>	Member tunnels of the aggregate. Tunnel name.	string	Maximum length: 79	
name	IPsec aggregate name.	string	Maximum length: 15	

config system ips-urlfilter-dns

Configure IPS URL filter DNS servers.

```
config system ips-urlfilter-dns
  Description: Configure IPS URL filter DNS servers.
  edit <address>
    set ipv6-capability [enable|disable]
    set status [enable|disable]
  next
end
```

config system ips-urlfilter-dns

Parameter	Description	Type	Size	Default						
address	DNS server IP address.	ipv4-address	Not Specified	0.0.0.0						
ipv6-capability	Enable/disable this server for IPv6 queries.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this DNS server for IPS URL filter DNS queries.</td></tr><tr><td>disable</td><td>Disable this DNS server for IPS URL filter DNS queries.</td></tr></table>				Option	Description	enable	Enable this DNS server for IPS URL filter DNS queries.	disable	Disable this DNS server for IPS URL filter DNS queries.
	Option	Description								
	enable	Enable this DNS server for IPS URL filter DNS queries.								
disable	Disable this DNS server for IPS URL filter DNS queries.									

config system ips-urlfilter-dns6

Configure IPS URL filter IPv6 DNS servers.

```
config system ips-urlfilter-dns6
  Description: Configure IPS URL filter IPv6 DNS servers.
  edit <address6>
    set status [enable|disable]
  next
end
```

config system ips-urlfilter-dns6

Parameter	Description	Type	Size	Default
address6	IPv6 address of DNS server.	ipv6-address	Not Specified	::
status	Enable/disable this server for IPv6 DNS queries.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	

config system ipv6-neighbor-cache

Configure IPv6 neighbor cache table.

```
config system ipv6-neighbor-cache
  Description: Configure IPv6 neighbor cache table.
  edit <id>
    set interface {string}
    set ipv6 {ipv6-address}
    set mac {mac-address}
  next
end
```


config system ipv6-neighbor-cache

Parameter	Description	Type	Size	Default
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Select the associated interface name from available options.	string	Maximum length: 15	
ipv6	IPv6 address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
mac	MAC address (format: xx:xx:xx:xx:xx:xx).	mac-address	Not Specified	00:00:00:00:00:00

config system ipv6-tunnel

Configure IPv6/IPv4 in IPv6 tunnel.

```
config system ipv6-tunnel
  Description: Configure IPv6/IPv4 in IPv6 tunnel.
  edit <name>
    set auto-asic-offload [enable|disable]
    set destination {ipv6-address}
    set interface {string}
    set source {ipv6-address}
    set use-sdwan [disable|enable]
  next
end
```

config system ipv6-tunnel

Parameter	Description	Type	Size	Default						
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auto ASIC offloading.</td></tr><tr><td><i>disable</i></td><td>Disable ASIC offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable auto ASIC offloading.	<i>disable</i>	Disable ASIC offloading.			
Option	Description									
<i>enable</i>	Enable auto ASIC offloading.									
<i>disable</i>	Disable ASIC offloading.									

Parameter	Description	Type	Size	Default
destination	Remote IPv6 address of the tunnel.	ipv6-address	Not Specified	::
interface	Interface name.	string	Maximum length: 15	
name	IPv6 tunnel name.	string	Maximum length: 15	
source	Local IPv6 address of the tunnel.	ipv6-address	Not Specified	::
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable

Option	Description
<i>disable</i>	Disable use of SD-WAN to reach remote gateway.
<i>enable</i>	Enable use of SD-WAN to reach remote gateway.

* This parameter may not exist in some models.

config system iscsi



This command is available for model(s): FortiGate-VM64 OPC.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure system iSCSI.

```
config system iscsi
  Description: Configure system iSCSI.
  edit <name>
    set ip {ipv4-address}
    set iqn {string}
    set port {integer}
  next
end
```

config system iscsi

Parameter	Description	Type	Size	Default
ip	iSCSI IP address.	ipv4-address	Not Specified	0.0.0.0
iqn	iSCSI qualified name.	string	Maximum length: 127	
name	iSCSI name.	string	Maximum length: 35	
port	iSCSI port number.	integer	Minimum value: 1 Maximum value: 65535	3260

config system isf-queue-profile



This command is available for model(s): FortiGate 1100E, FortiGate 1101E, FortiGate 1800F, FortiGate 1801F, FortiGate 2200E, FortiGate 2201E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3700D, FortiGate 400E, FortiGate 401E, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 800D.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 120G, FortiGate 121G, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2500E, FortiGate 3000F, FortiGate 3001F, FortiGate 3200F, FortiGate 3201F, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400F, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Create a queue profile of switch.

```
config system isf-queue-profile
  Description: Create a queue profile of switch.
  edit <name>
    set bandwidth-unit [kbps|pps]
    set burst-bps-granularity [disable|512-bytes|...]
    set burst-pps-granularity [disable|half-packet|...]
    set guaranteed-bandwidth {integer}
    set maximum-bandwidth {integer}
  next
end
```

config system isf-queue-profile

Parameter	Description	Type	Size	Default
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth.	option	-	kbps

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>kbps</i>	kilobits per second.		
	<i>pps</i>	packets per second.		
burst-bps-granularity	Burst granularity based on bytes per second.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable burst control.		
	<i>512-bytes</i>	512 bytes.		
	<i>1k-bytes</i>	1K bytes.		
	<i>2k-bytes</i>	2K bytes.		
	<i>4k-bytes</i>	4K bytes.		
	<i>8k-bytes</i>	8K bytes.		
	<i>16k-bytes</i>	16K bytes.		
	<i>32k-bytes</i>	32K bytes.		
burst-pps-granularity	Burst granularity based on packets per second.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable burst control.		
	<i>half-packet</i>	One burst unit equals two time slots in which one packet is sent.		
	<i>1-packet</i>	1 packet.		
	<i>2-packets</i>	2 packets.		
	<i>4-packets</i>	4 packets.		
	<i>16-packets</i>	16 packets.		
	<i>65-packets</i>	65 packets.		
	<i>262-packets</i>	262 packets.		
guaranteed-bandwidth	Guaranteed bandwidth.	integer	Minimum value: 0 Maximum value: 1000000000	0

Parameter	Description	Type	Size	Default
maximum-bandwidth	Upper bandwidth limit enforced.	integer	Minimum value: 0 Maximum value: 1000000000	0
name	Profile name.	string	Maximum length: 15	

config system link-monitor

Configure Link Health Monitor.

```

config system link-monitor
  Description: Configure Link Health Monitor.
  edit <name>
    set addr-mode [ipv4|ipv6]
    set class-id {integer}
    set diffservcode {user}
    set fail-weight {integer}
    set failtime {integer}
    set gateway-ip {ipv4-address-any}
    set gateway-ip6 {ipv6-address}
    set ha-priority {integer}
    set http-agent {string}
    set http-get {string}
    set http-match {string}
    set interval {integer}
    set packet-size {integer}
    set password {password}
    set port {integer}
    set probe-count {integer}
    set probe-timeout {integer}
    set protocol {option1}, {option2}, ...
    set recoverytime {integer}
    set route <subnet1>, <subnet2>, ...
    set security-mode [none|authentication]
    set server <address1>, <address2>, ...
    set server-config [default|individual]
  config server-list
    Description: Servers for link-monitor to monitor.
    edit <id>
      set dst {string}
      set port {integer}
      set protocol {option1}, {option2}, ...
      set weight {integer}
    next
  end

```

```

set server-type [static|dynamic]
set service-detection [enable|disable]
set source-ip {ipv4-address-any}
set source-ip6 {ipv6-address}
set srcintf {string}
set status [enable|disable]
set update-cascade-interface [enable|disable]
set update-policy-route [enable|disable]
set update-static-route [enable|disable]
next
end

```

config system link-monitor

Parameter	Description	Type	Size	Default						
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 mode.</td></tr><tr><td>ipv6</td><td>IPv6 mode.</td></tr></table>	Option	Description	ipv4	IPv4 mode.	ipv6	IPv6 mode.			
	Option	Description								
	ipv4	IPv4 mode.								
ipv6	IPv6 mode.									
class-id	Traffic class ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0						
diffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified							
fail-weight	Threshold weight to trigger link failure alert.	integer	Minimum value: 0 0 Maximum value: 255	0						
failtime	Number of retry attempts before the server is considered down (1 - 3600, default = 5).	integer	Minimum value: 1 1 Maximum value: 3600	5						
gateway-ip	Gateway IP address used to probe the server.	ipv4-address-any	Not Specified	0.0.0.0						
gateway-ip6	Gateway IPv6 address used to probe the server.	ipv6-address	Not Specified	::						
ha-priority	HA election priority (1 - 50).	integer	Minimum value: 1 1 Maximum value: 50	1						

Parameter	Description	Type	Size	Default														
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/														
http-get	If you are monitoring an HTML server you can send an HTTP-GET request with a custom string. Use this option to define the string.	string	Maximum length: 1024	/														
http-match	String that you expect to see in the HTTP-GET requests of the traffic to be monitored.	string	Maximum length: 1024															
interval	Detection interval in milliseconds (20 - 3600 * 1000 msec, default = 500).	integer	Minimum value: 20 Maximum value: 3600000	500														
name	Link monitor name.	string	Maximum length: 35															
packet-size	Packet size of a TWAMP test session (124/158 - 1024).	integer	Minimum value: 124 0 Maximum value: 65535	124														
password	TWAMP controller password in authentication mode.	password	Not Specified															
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0														
probe-count	Number of most recent probes that should be used to calculate latency and jitter (5 - 30, default = 30).	integer	Minimum value: 5 Maximum value: 30	30														
probe-timeout	Time to wait before a probe packet is considered lost (20 - 5000 msec, default = 500).	integer	Minimum value: 20 Maximum value: 5000	500														
protocol	Protocols used to monitor the server.	option	-	ping														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING link monitor.</td></tr><tr><td>tcp-echo</td><td>TCP echo link monitor.</td></tr><tr><td>udp-echo</td><td>UDP echo link monitor.</td></tr><tr><td>http</td><td>HTTP-GET link monitor.</td></tr><tr><td>https</td><td>HTTPS-GET link monitor.</td></tr><tr><td>twamp</td><td>TWAMP link monitor.</td></tr></table>				Option	Description	ping	PING link monitor.	tcp-echo	TCP echo link monitor.	udp-echo	UDP echo link monitor.	http	HTTP-GET link monitor.	https	HTTPS-GET link monitor.	twamp	TWAMP link monitor.
Option	Description																	
ping	PING link monitor.																	
tcp-echo	TCP echo link monitor.																	
udp-echo	UDP echo link monitor.																	
http	HTTP-GET link monitor.																	
https	HTTPS-GET link monitor.																	
twamp	TWAMP link monitor.																	

Parameter	Description	Type	Size	Default						
recoverytime	Number of successful responses received before server is considered recovered (1 - 3600, default = 5).	integer	Minimum value: 1 Maximum value: 3600	5						
route <subnet>	Subnet to monitor. IP and netmask (x.x.x.x/y).	string	Maximum length: 79							
security-mode	Twamp controller security mode.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Unauthenticated mode.</td></tr><tr><td>authentication</td><td>Authenticated mode.</td></tr></table>				Option	Description	none	Unauthenticated mode.	authentication	Authenticated mode.
Option	Description									
none	Unauthenticated mode.									
authentication	Authenticated mode.									
server <address>	IP address of the server(s) to be monitored. Server address.	string	Maximum length: 79							
server-config	Mode of server configuration.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>All servers share the same attributes.</td></tr><tr><td>individual</td><td>Some attributes can be specified for individual servers.</td></tr></table>				Option	Description	default	All servers share the same attributes.	individual	Some attributes can be specified for individual servers.
Option	Description									
default	All servers share the same attributes.									
individual	Some attributes can be specified for individual servers.									
server-type	Server type (static or dynamic).	option	-	static						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Static servers.</td></tr><tr><td>dynamic</td><td>Dynamic servers.</td></tr></table>				Option	Description	static	Static servers.	dynamic	Dynamic servers.
Option	Description									
static	Static servers.									
dynamic	Dynamic servers.									
service-detection	Only use monitor to read quality values. If enabled, static routes and cascade interfaces will not be updated.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Only use monitor for service-detection.</td></tr><tr><td>disable</td><td>Monitor will update routes/interfaces on link failure.</td></tr></table>				Option	Description	enable	Only use monitor for service-detection.	disable	Monitor will update routes/interfaces on link failure.
Option	Description									
enable	Only use monitor for service-detection.									
disable	Monitor will update routes/interfaces on link failure.									
source-ip	Source IP address used in packet to the server.	ipv4-address-any	Not Specified	0.0.0.0						
source-ip6	Source IPv6 address used in packet to the server.	ipv6-address	Not Specified	::						
srcintf	Interface that receives the traffic to be monitored.	string	Maximum length: 15							

Parameter	Description	Type	Size	Default
status	Enable/disable this link monitor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this link monitor.		
	<i>disable</i>	Disable this link monitor.		
update-cascade-interface	Enable/disable update cascade interface.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable update cascade interface.		
	<i>disable</i>	Disable update cascade interface.		
update-policy-route	Enable/disable updating the policy route.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable updating the policy route.		
	<i>disable</i>	Disable updating the policy route.		
update-static-route	Enable/disable updating the static route.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable updating the static route.		
	<i>disable</i>	Disable updating the static route.		

config server-list

Parameter	Description	Type	Size	Default
dst	IP address of the server to be monitored.	string	Maximum length: 64	
id	Server ID.	integer	Minimum value: 1 Maximum value: 32	0

Parameter	Description	Type	Size	Default
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0
protocol	Protocols used to monitor the server.	option	-	ping
	Option Description			
	<i>ping</i>	PING link monitor.		
	<i>tcp-echo</i>	TCP echo link monitor.		
	<i>udp-echo</i>	UDP echo link monitor.		
	<i>http</i>	HTTP-GET link monitor.		
	<i>https</i>	HTTPS-GET link monitor.		
	<i>twamp</i>	TWAMP link monitor.		
weight	Weight of the monitor to this dst (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0

config system lldp network-policy

Configure LLDP network policy.

```

config system lldp network-policy
  Description: Configure LLDP network policy.
  edit <name>
    set comment {var-string}
    config guest
      Description: Guest.
      set dscp {integer}
      set priority {integer}
      set status [disable|enable]
      set tag [none|dot1q|...]
      set vlan {integer}
    end
    config guest-voice-signaling
      Description: Guest Voice Signaling.
      set dscp {integer}
      set priority {integer}
      set status [disable|enable]
      set tag [none|dot1q|...]
      set vlan {integer}
  
```

```

end
config softphone
    Description: Softphone.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config streaming-video
    Description: Streaming Video.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config video-conferencing
    Description: Video Conferencing.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config video-signaling
    Description: Video Signaling.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config voice
    Description: Voice.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config voice-signaling
    Description: Voice signaling.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
next
end

```

config system lldp network-policy

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
name	LLDP network policy name.	string	Maximum length: 35	

config guest

Parameter	Description	Type	Size	Default								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	5								
status	Enable/disable advertising this policy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable advertising this LLDP network policy.</td></tr><tr><td>enable</td><td>Enable advertising this LLDP network policy.</td></tr></table>	Option	Description	disable	Disable advertising this LLDP network policy.	enable	Enable advertising this LLDP network policy.					
Option	Description											
disable	Disable advertising this LLDP network policy.											
enable	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Advertise that untagged frames should be used.</td></tr><tr><td>dot1q</td><td>Advertise that 802.1Q (VLAN) tagging should be used.</td></tr><tr><td>dot1p</td><td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td></tr></table>	Option	Description	none	Advertise that untagged frames should be used.	dot1q	Advertise that 802.1Q (VLAN) tagging should be used.	dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
none	Advertise that untagged frames should be used.											
dot1q	Advertise that 802.1Q (VLAN) tagging should be used.											
dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0								

config guest-voice-signaling

Parameter	Description	Type	Size	Default
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	5
status	Enable/disable advertising this policy.	option	-	disable
		Option	Description	
		<i>disable</i>	Disable advertising this LLDP network policy.	
		<i>enable</i>	Enable advertising this LLDP network policy.	
tag	Advertise tagged or untagged traffic.	option	-	none
		Option	Description	
		<i>none</i>	Advertise that untagged frames should be used.	
		<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	
		<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.	
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0

config softphone

Parameter	Description	Type	Size	Default
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	5
status	Enable/disable advertising this policy.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	Option	Description		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0

config streaming-video

Parameter	Description	Type	Size	Default								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	5								
status	Enable/disable advertising this policy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable advertising this LLDP network policy.</td></tr><tr><td>enable</td><td>Enable advertising this LLDP network policy.</td></tr></table>				Option	Description	disable	Disable advertising this LLDP network policy.	enable	Enable advertising this LLDP network policy.		
Option	Description											
disable	Disable advertising this LLDP network policy.											
enable	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Advertise that untagged frames should be used.</td></tr><tr><td>dot1q</td><td>Advertise that 802.1Q (VLAN) tagging should be used.</td></tr><tr><td>dot1p</td><td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td></tr></table>				Option	Description	none	Advertise that untagged frames should be used.	dot1q	Advertise that 802.1Q (VLAN) tagging should be used.	dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.
Option	Description											
none	Advertise that untagged frames should be used.											
dot1q	Advertise that 802.1Q (VLAN) tagging should be used.											
dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.											

Parameter	Description	Type	Size	Default
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0

config video-conferencing

Parameter	Description	Type	Size	Default								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	5								
status	Enable/disable advertising this policy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable advertising this LLDP network policy.</td></tr><tr><td>enable</td><td>Enable advertising this LLDP network policy.</td></tr></table>				Option	Description	disable	Disable advertising this LLDP network policy.	enable	Enable advertising this LLDP network policy.		
Option	Description											
disable	Disable advertising this LLDP network policy.											
enable	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Advertise that untagged frames should be used.</td></tr><tr><td>dot1q</td><td>Advertise that 802.1Q (VLAN) tagging should be used.</td></tr><tr><td>dot1p</td><td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td></tr></table>				Option	Description	none	Advertise that untagged frames should be used.	dot1q	Advertise that 802.1Q (VLAN) tagging should be used.	dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.
Option	Description											
none	Advertise that untagged frames should be used.											
dot1q	Advertise that 802.1Q (VLAN) tagging should be used.											
dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0								

config video-signaling

Parameter	Description	Type	Size	Default
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

Parameter	Description	Type	Size	Default
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	5
status	Enable/disable advertising this policy.	option	-	disable
	Option	Description		
	disable	Disable advertising this LLDP network policy.		
	enable	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	Option	Description		
	none	Advertise that untagged frames should be used.		
	dot1q	Advertise that 802.1Q (VLAN) tagging should be used.		
	dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0

config voice

Parameter	Description	Type	Size	Default						
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46						
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	5						
status	Enable/disable advertising this policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable advertising this LLDP network policy.</td></tr><tr><td>enable</td><td>Enable advertising this LLDP network policy.</td></tr></table>				Option	Description	disable	Disable advertising this LLDP network policy.	enable	Enable advertising this LLDP network policy.
Option	Description									
disable	Disable advertising this LLDP network policy.									
enable	Enable advertising this LLDP network policy.									
tag	Advertise tagged or untagged traffic.	option	-	none						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0

config voice-signaling

Parameter	Description	Type	Size	Default
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7	5
status	Enable/disable advertising this policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	Option	Description		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0

config system lte-modem



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

Configure USB LTE/WIMAX devices.

```
config system lte-modem
  Description: Configure USB LTE/WIMAX devices.
  set allow-modify-mtu-size [enable|disable]
  set allow-modify-wireless-profile-table [enable|disable]
  set apn {string}
  set authtype [none|pap|...]
  set auto-connect [enable|disable]
  set band-restrictions {string}
  config data-plan
    Description: Configure data plan.
    edit <name>
      set billing-date {integer}
      set billing-hour {integer}
      set billing-period [monthly|weekly|...]
      set billing-weekday [sunday|monday|...]
      set data-limit {integer}
      set data-limit-alert {integer}
      set delay-switch-time {string}
      set iccid {string}
      set overage [enable|disable]
      set target-sim-slot [SIM-slot-1|SIM-slot-2]
    next
  next
```

```

end
set data-usage-tracking [enable|disable]
set dhcp-relay [enable|disable]
set extra-init {string}
set force-wireless-profile {integer}
set gps-port {integer}
set gps-service [enable|disable]
set holddown-timer {integer}
set image-preference [generic|att|...]
set interface {string}
set manual-handover [enable|disable]
set mode [standalone|redundant]
set modem-port {integer}
set network-type [auto|umts-3g|...]
set override-gateway [enable|disable]
set passwd {password}
set pdptype {option}
config sim-switch
    Description: Configure SIM card switch.
    set by-connection-state [disable|enable]
    set by-data-plan [enable|disable]
    set by-link-monitor [disable|enable]
    set by-sim-state [disable|enable]
    set link-monitor {string}
    set modem-disconnection-time {integer}
    set sim-slot {integer}
    set sim-switch-log-alert-interval {integer}
    set sim-switch-log-alert-threshold {integer}
end
set sim1-pin {password}
set sim2-pin {password}
set status [enable|disable]
set username {string}
end

```

config system lte-modem

Parameter	Description	Type	Size	Default						
allow-modify-mtu-size *	Allow FortiGate to modify the wireless WAN interface MTU size.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow LTE daemon to modify wireless profile table.</td></tr><tr><td>disable</td><td>Do not allow LTE daemon to modify wireless profile table.</td></tr></table>				Option	Description	enable	Allow LTE daemon to modify wireless profile table.	disable	Do not allow LTE daemon to modify wireless profile table.
Option	Description									
enable	Allow LTE daemon to modify wireless profile table.									
disable	Do not allow LTE daemon to modify wireless profile table.									

Parameter	Description	Type	Size	Default								
allow-modify-wireless-profile-table *	Allow FortiGate to modify the wireless profile table if the internal LTE modem is running the GENERIC modem firmware.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow LTE daemon to modify wireless profile table.</td></tr><tr><td>disable</td><td>Do not allow LTE daemon to modify wireless profile table.</td></tr></table>	Option	Description	enable	Allow LTE daemon to modify wireless profile table.	disable	Do not allow LTE daemon to modify wireless profile table.					
Option	Description											
enable	Allow LTE daemon to modify wireless profile table.											
disable	Do not allow LTE daemon to modify wireless profile table.											
apn	Login APN string for PDP-IP packet data calls.	string	Maximum length: 127									
authtype	Authentication type for PDP-IP packet data calls.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Username and password not required.</td></tr><tr><td>pap</td><td>Use PAP authentication.</td></tr><tr><td>chap</td><td>Use CHAP authentication.</td></tr></table>	Option	Description	none	Username and password not required.	pap	Use PAP authentication.	chap	Use CHAP authentication.			
Option	Description											
none	Username and password not required.											
pap	Use PAP authentication.											
chap	Use CHAP authentication.											
auto-connect *	Enable/disable modem auto connect.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable modem auto connect.</td></tr><tr><td>disable</td><td>Disable modem auto connect.</td></tr></table>	Option	Description	enable	Enable modem auto connect.	disable	Disable modem auto connect.					
Option	Description											
enable	Enable modem auto connect.											
disable	Disable modem auto connect.											
band-restrictions *	Bitmaps for the allowed 3G and LTE bands.Ex: 0000000000000000-0000000000001008 (3G Mask-LTE Mask)	string	Maximum length: 35									
data-usage-tracking *	Enable/disable data usage tracking.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable data usage tracking.</td></tr><tr><td>disable</td><td>Disable data usage tracking.</td></tr></table>	Option	Description	enable	Enable data usage tracking.	disable	Disable data usage tracking.					
Option	Description											
enable	Enable data usage tracking.											
disable	Disable data usage tracking.											
dhcp-relay *	Enable/disable DHCP relay over modem.	option	-	disable								

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP relay.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP relay.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP relay.	<i>disable</i>	Disable DHCP relay.																	
	Option	Description																						
	<i>enable</i>	Enable DHCP relay.																						
<i>disable</i>	Disable DHCP relay.																							
extra-init	Extra initialization string for USB LTE/WIMAX devices.	string	Maximum length: 127																					
force-wireless-profile *	Force to use wireless profile index (1 - 16), 0 if don't force.	integer	Minimum value: 0 Maximum value: 16	0																				
gps-port *	Modem GPS port index (0 - 20).	integer	Minimum value: 0 Maximum value: 20	255																				
gps-service *	Enable/disable GPS daemon.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GPS daemon.</td></tr><tr><td><i>disable</i></td><td>Disable GPS daemon.</td></tr></table>	Option	Description	<i>enable</i>	Enable GPS daemon.	<i>disable</i>	Disable GPS daemon.																	
	Option	Description																						
	<i>enable</i>	Enable GPS daemon.																						
<i>disable</i>	Disable GPS daemon.																							
holddown-timer	Hold down timer (10 - 60 sec).	integer	Minimum value: 10 Maximum value: 60	30																				
image-preference *	Modem Image Preference.	option	-	auto-sim																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>generic</i></td><td>Generic Firmware.</td></tr><tr><td><i>att</i></td><td>AT&T Firmware.</td></tr><tr><td><i>verizon</i></td><td>Verizon Firmware.</td></tr><tr><td><i>telus</i></td><td>Telus Firmware.</td></tr><tr><td><i>docomo</i></td><td>DOCOMO Firmware.</td></tr><tr><td><i>softbank</i></td><td>Softbank Firmware.</td></tr><tr><td><i>sprint</i></td><td>Sprint Firmware.</td></tr><tr><td><i>auto-sim</i></td><td>Auto Select Firmware.</td></tr><tr><td><i>no-change</i></td><td>Do not change.</td></tr></table>	Option	Description	<i>generic</i>	Generic Firmware.	<i>att</i>	AT&T Firmware.	<i>verizon</i>	Verizon Firmware.	<i>telus</i>	Telus Firmware.	<i>docomo</i>	DOCOMO Firmware.	<i>softbank</i>	Softbank Firmware.	<i>sprint</i>	Sprint Firmware.	<i>auto-sim</i>	Auto Select Firmware.	<i>no-change</i>	Do not change.			
	Option	Description																						
	<i>generic</i>	Generic Firmware.																						
	<i>att</i>	AT&T Firmware.																						
	<i>verizon</i>	Verizon Firmware.																						
	<i>telus</i>	Telus Firmware.																						
	<i>docomo</i>	DOCOMO Firmware.																						
	<i>softbank</i>	Softbank Firmware.																						
	<i>sprint</i>	Sprint Firmware.																						
	<i>auto-sim</i>	Auto Select Firmware.																						
<i>no-change</i>	Do not change.																							

Parameter	Description	Type	Size	Default								
interface	The interface that the modem is acting as a redundant interface for.	string	Maximum length: 63									
manual-handover *	Enable/Disable manual handover from 3G to LTE network.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 3G to LTE manual handover.</td></tr><tr><td><i>disable</i></td><td>Disable 3G to LTE manual handover.</td></tr></table>	Option	Description	<i>enable</i>	Enable 3G to LTE manual handover.	<i>disable</i>	Disable 3G to LTE manual handover.					
Option	Description											
<i>enable</i>	Enable 3G to LTE manual handover.											
<i>disable</i>	Disable 3G to LTE manual handover.											
mode	Modem operation mode.	option	-	standalone								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standalone</i></td><td>Standalone modem operation mode.</td></tr><tr><td><i>redundant</i></td><td>Redundant modem operation mode where the modem is used as a backup interface.</td></tr></table>	Option	Description	<i>standalone</i>	Standalone modem operation mode.	<i>redundant</i>	Redundant modem operation mode where the modem is used as a backup interface.					
Option	Description											
<i>standalone</i>	Standalone modem operation mode.											
<i>redundant</i>	Redundant modem operation mode where the modem is used as a backup interface.											
modem-port	Modem port index (0 - 20).	integer	Minimum value: 0 Maximum value: 20	255								
network-type *	Wireless network type.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatic detection</td></tr><tr><td><i>umts-3g</i></td><td>UMTS 3G -- For networks use GSM technology</td></tr><tr><td><i>lte</i></td><td>LTE</td></tr></table>	Option	Description	<i>auto</i>	Automatic detection	<i>umts-3g</i>	UMTS 3G -- For networks use GSM technology	<i>lte</i>	LTE			
Option	Description											
<i>auto</i>	Automatic detection											
<i>umts-3g</i>	UMTS 3G -- For networks use GSM technology											
<i>lte</i>	LTE											
override-gateway *	Enable/disable LTE gateway override (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override gateway to 0.0.0.0</td></tr><tr><td><i>disable</i></td><td>Use gateway as assigned by ISP DHCP server.</td></tr></table>	Option	Description	<i>enable</i>	Override gateway to 0.0.0.0	<i>disable</i>	Use gateway as assigned by ISP DHCP server.					
Option	Description											
<i>enable</i>	Override gateway to 0.0.0.0											
<i>disable</i>	Use gateway as assigned by ISP DHCP server.											
passwd	Authentication password for PDP-IP packet data calls.	password	Not Specified									
pdptype	Packet Data Protocol (PDP) context type.	option	-	**								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>IPv4</i>	Only IPv4.		
sim1-pin *	PIN code for SIM #1 (if applicable).	password	Not Specified	
sim2-pin *	PIN code for SIM #2 (if applicable).	password	Not Specified	
status	Enable/disable USB LTE/WIMAX device.	option	-	disable **
	Option	Description		
	<i>enable</i>	Enable USB LTE/WIMA device.		
	<i>disable</i>	Disable USB LTE/WIMA device.		
username	Authentication username for PDP-IP packet data calls.	string	Maximum length: 63	

* This parameter may not exist in some models.

** Values may differ between models.

config data-plan

Parameter	Description	Type	Size	Default
billing-date	LTE MODEM billing date (1 - 31).	integer	Minimum value: 1 Maximum value: 31	4294967295
billing-hour	LTE MODEM billing hour (0 - 23).	integer	Minimum value: 0 Maximum value: 23	4294967295
billing-period	<MONTH, WEEK, DAY>	option	-	
	Option	Description		
	<i>monthly</i>	1-31(day)		
	<i>weekly</i>	Mon to Sun		
	<i>daily</i>	1-24(hour)		
billing-weekday	LTE MODEM billing weekday (Mon - Sun).	option	-	

Parameter	Description	Type	Size	Default
	Option Description			
	<i>sunday</i>	Sunday		
	<i>monday</i>	Monday		
	<i>tuesday</i>	Tuesday		
	<i>wednesday</i>	Wednesday		
	<i>thursday</i>	Thursday		
	<i>friday</i>	Friday		
	<i>saturday</i>	Saturday		
data-limit	LTE MODEM data limit in megabytes (0 - 100000, use zero for unlimited data).	integer	Minimum value: 0 Maximum value: 100000	4294967295
data-limit-alert	LTE MODEM data usage percentage at which to trigger log. (1 - 99 percent, default = 75).	integer	Minimum value: 1 Maximum value: 99	75
delay-switch-time	Instead of SIM switching shortly after data limit is reached, schedule a delay switch time in format hh:mm.	string	Maximum length: 35	NA
iccid	Dedicated data plan to specific ICCID.	string	Maximum length: 35	
name	Data plan name.	string	Maximum length: 35	
overage	Enable/disable allowance of data overage as configured by data-limit (default = enable). If disabled, perform sim-swap/stop-network as configured by by-data-plan.	option	-	enable
	Option Description			
	<i>enable</i>	Allow data overage data-limit. This won't perform sim-swap/stop-network.		
	<i>disable</i>	Disable data overage data-limit. This will perform sim-swap/stop-network as configured by by-data-plan.		
target-sim-slot	Target sim slot <1 or 2>	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>SIM-slot-1</i>	SIM slot 1		
	<i>SIM-slot-2</i>	SIM slot 2		

config sim-switch

Parameter	Description	Type	Size	Default
by-connection-state	Enable/disable automatic switch of SIM by MODEM connection state (mobile data usage charges not incurred).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SIM auto switch by modem connection state.		
	<i>enable</i>	Enable SIM auto switch by modem connection state.		
by-data-plan	Enable/disable SIM auto switch by data-plan config.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatic switch of SIM by data-plan configuration.		
	<i>disable</i>	Disable automatic switch of SIM by data-plan configuration.		
by-link-monitor	Enable/disable automatic switch of SIM by link monitor (mobile data usage charges incurred).	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SIM auto switch by link monitor.		
	<i>enable</i>	Enable SIM auto switch by link monitor.		
by-sim-state	Enable/disable automatic switch of SIM when MODEM SIM state is empty or in error.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SIM auto switch when SIM state is empty or in error.		
	<i>enable</i>	Enable SIM auto switch when SIM state is empty or in error.		
link-monitor	Set link monitor name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
modem-disconnection-time	Configure connection-based automatic switch of SIM time interval in seconds (30 - 86400).	integer	Minimum value: 30 Maximum value: 86400	300
sim-slot	SIM card slot (1 - 2). 1: SIM-slot 1. 2: SIM-slot 2.	integer	Minimum value: 1 Maximum value: 2	1
sim-switch-log-alert-interval	When sim-switch > X threshold within Y interval, trigger log event (Y:1 - 99999 min, default = 15).	integer	Minimum value: 1 Maximum value: 99999	15
sim-switch-log-alert-threshold	When sim-switch > X threshold within Y interval, trigger log event (X:1 - 1000 times, default = 5).	integer	Minimum value: 1 Maximum value: 1000	5

config system mac-address-table

Configure MAC address tables.

```

config system mac-address-table
  Description: Configure MAC address tables.
  edit <mac>
    set interface {string}
    set reply-substitute {mac-address}
  next
end

```

config system mac-address-table

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 35	
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
reply-substitute	New MAC for reply traffic.	mac-address	Not Specified	00:00:00:00:00:00

config system management-tunnel

Management tunnel configuration.

```
config system management-tunnel
  Description: Management tunnel configuration.
  set allow-collect-statistics [enable|disable]
  set allow-config-restore [enable|disable]
  set allow-push-configuration [enable|disable]
  set allow-push-firmware [enable|disable]
  set authorized-manager-only [enable|disable]
  set serial-number {user}
  set status [enable|disable]
end
```

config system management-tunnel

Parameter	Description	Type	Size	Default
allow-collect-statistics	Enable/disable collection of run time statistics.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable collection of run time statistics.		
	<i>disable</i>	Disable collection of run time statistics.		
allow-config-restore	Enable/disable allow config restore.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable allow config restore.		
	<i>disable</i>	Disable allow config restore.		
allow-push-configuration	Enable/disable push configuration.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable push configuration.		
	<i>disable</i>	Disable push configuration.		
allow-push-firmware	Enable/disable push firmware.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable push firmware.		
	<i>disable</i>	Disable push firmware.		
authorized-manager-only	Enable/disable restriction of authorized manager only.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable restriction of authorized manager only.		
	<i>disable</i>	Disable restriction of authorized manager only.		
serial-number	Serial number.	user	Not Specified	
status	Enable/disable FGFM tunnel.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable management tunnel.		
	<i>disable</i>	Disable management tunnel.		

config system mobile-tunnel

Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions for Mobile IPv4 RFC5177.

```

config system mobile-tunnel
    Description: Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions
    for Mobile IPv4 RFC5177.
    edit <name>
        set hash-algorithm {option}
        set home-address {ipv4-address}
        set home-agent {ipv4-address}
        set lifetime {integer}
        set n-mhae-key {password_aes256}
        set n-mhae-key-type [ascii|base64]
        set n-mhae-spi {integer}
    config network
        Description: NEMO network configuration.
        edit <id>
            set interface {string}
            set prefix {ipv4-classnet}
        next
    end
    set reg-interval {integer}
    set reg-retry {integer}

```

```

    set renew-interval {integer}
    set roaming-interface {string}
    set status [disable|enable]
    set tunnel-mode {option}
next
end

```

config system mobile-tunnel

Parameter	Description	Type	Size	Default						
hash-algorithm	Hash Algorithm (Keyed MD5).	option	-	hmac-md5						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hmac-md5</td><td>Keyed MD5.</td></tr></table>	Option	Description	hmac-md5	Keyed MD5.					
Option	Description									
hmac-md5	Keyed MD5.									
home-address	Home IP address (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0						
home-agent	IPv4 address of the NEMO HA (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0						
lifetime	NMMO HA registration request lifetime (180 - 65535 sec, default = 65535).	integer	Minimum value: 180 Maximum value: 65535	65535						
n-mhae-key	NEMO authentication key.	password_aes256	Not Specified							
n-mhae-key-type	NEMO authentication key type (ASCII or base64).	option	-	ascii						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ascii</td><td>The authentication key is an ASCII string.</td></tr><tr><td>base64</td><td>The authentication key is Base64 encoded.</td></tr></table>	Option	Description	ascii	The authentication key is an ASCII string.	base64	The authentication key is Base64 encoded.			
Option	Description									
ascii	The authentication key is an ASCII string.									
base64	The authentication key is Base64 encoded.									
n-mhae-spi	NEMO authentication SPI (default: 256).	integer	Minimum value: 0 Maximum value: 4294967295	256						
name	Tunnel name.	string	Maximum length: 15							
reg-interval	NMMO HA registration interval (5 - 300, default = 5).	integer	Minimum value: 5 Maximum value: 300	5						

Parameter	Description	Type	Size	Default						
reg-retry	Maximum number of NMMO HA registration retries (1 to 30, default = 3).	integer	Minimum value: 1 Maximum value: 30	3						
renew-interval	Time before lifetime expiration to send NMMO HA re-registration (5 - 60, default = 60).	integer	Minimum value: 5 Maximum value: 60	60						
roaming-interface	Select the associated interface name from available options.	string	Maximum length: 15							
status	Enable/disable this mobile tunnel.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable this mobile tunnel.</td></tr><tr><td>enable</td><td>Enable this mobile tunnel.</td></tr></table>				Option	Description	disable	Disable this mobile tunnel.	enable	Enable this mobile tunnel.
Option	Description									
disable	Disable this mobile tunnel.									
enable	Enable this mobile tunnel.									
tunnel-mode	NEMO tunnel mode (GRE tunnel).	option	-	gre						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>gre</td><td>GRE tunnel.</td></tr></table>				Option	Description	gre	GRE tunnel.		
Option	Description									
gre	GRE tunnel.									

config network

Parameter	Description	Type	Size	Default
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Select the associated interface name from available options.	string	Maximum length: 15	
prefix	Class IP and Netmask with correction (Format:xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/x).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config system modem



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

Configure MODEM.

```
config system modem
  Description: Configure MODEM.
  set action [dial|stop|...]
  set altmode [enable|disable]
  set authtype1 {option1}, {option2}, ...
  set authtype2 {option1}, {option2}, ...
  set authtype3 {option1}, {option2}, ...
  set auto-dial [enable|disable]
  set connect-timeout {integer}
  set dial-cmd1 {string}
  set dial-cmd2 {string}
  set dial-cmd3 {string}
  set dial-on-demand [enable|disable]
  set distance {integer}
  set dont-send-CR1 [enable|disable]
  set dont-send-CR2 [enable|disable]
  set dont-send-CR3 [enable|disable]
  set extra-init1 {string}
  set extra-init2 {string}
  set extra-init3 {string}
  set holddown-timer {integer}
  set idle-timer {integer}
```



```

set interface {string}
set lockdown-lac {string}
set mode [standalone|redundant]
set network-init {string}
set passwd1 {password}
set passwd2 {password}
set passwd3 {password}
set peer-modem1 [generic|actiontec|...]
set peer-modem2 [generic|actiontec|...]
set peer-modem3 [generic|actiontec|...]
set phone1 {string}
set phone2 {string}
set phone3 {string}
set pin-init {string}
set ppp-echo-request1 [enable|disable]
set ppp-echo-request2 [enable|disable]
set ppp-echo-request3 [enable|disable]
set priority {integer}
set redial [none|1|...]
set reset {integer}
set status [enable|disable]
set traffic-check [enable|disable]
set username1 {string}
set username2 {string}
set username3 {string}
set wireless-port {integer}
end

```

config system modem

Parameter	Description	Type	Size	Default								
action	Dial up/stop MODEM.	option	-	stop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dial</td><td>Dial up number.</td></tr><tr><td>stop</td><td>Stop dialup.</td></tr><tr><td>none</td><td>No action.</td></tr></table>				Option	Description	dial	Dial up number.	stop	Stop dialup.	none	No action.
	Option	Description										
	dial	Dial up number.										
	stop	Stop dialup.										
none	No action.											
altmode	Enable/disable altmode for installations using PPP in China.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.		
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											

Parameter	Description	Type	Size	Default										
authtype1	Allowed authentication types for ISP 1.	option	-	pap chap mschap mschapv2										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pap</i></td><td>PAP</td></tr><tr><td><i>chap</i></td><td>CHAP</td></tr><tr><td><i>mschap</i></td><td>MSCHAP</td></tr><tr><td><i>mschapv2</i></td><td>MSCHAPv2</td></tr></table>	Option	Description	<i>pap</i>	PAP	<i>chap</i>	CHAP	<i>mschap</i>	MSCHAP	<i>mschapv2</i>	MSCHAPv2			
Option	Description													
<i>pap</i>	PAP													
<i>chap</i>	CHAP													
<i>mschap</i>	MSCHAP													
<i>mschapv2</i>	MSCHAPv2													
authtype2	Allowed authentication types for ISP 2.	option	-	pap chap mschap mschapv2										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pap</i></td><td>PAP</td></tr><tr><td><i>chap</i></td><td>CHAP</td></tr><tr><td><i>mschap</i></td><td>MSCHAP</td></tr><tr><td><i>mschapv2</i></td><td>MSCHAPv2</td></tr></table>	Option	Description	<i>pap</i>	PAP	<i>chap</i>	CHAP	<i>mschap</i>	MSCHAP	<i>mschapv2</i>	MSCHAPv2			
Option	Description													
<i>pap</i>	PAP													
<i>chap</i>	CHAP													
<i>mschap</i>	MSCHAP													
<i>mschapv2</i>	MSCHAPv2													
authtype3	Allowed authentication types for ISP 3.	option	-	pap chap mschap mschapv2										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pap</i></td><td>PAP</td></tr><tr><td><i>chap</i></td><td>CHAP</td></tr><tr><td><i>mschap</i></td><td>MSCHAP</td></tr><tr><td><i>mschapv2</i></td><td>MSCHAPv2</td></tr></table>	Option	Description	<i>pap</i>	PAP	<i>chap</i>	CHAP	<i>mschap</i>	MSCHAP	<i>mschapv2</i>	MSCHAPv2			
Option	Description													
<i>pap</i>	PAP													
<i>chap</i>	CHAP													
<i>mschap</i>	MSCHAP													
<i>mschapv2</i>	MSCHAPv2													
auto-dial	Enable/disable auto-dial after a reboot or disconnection.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
connect-timeout	Connection completion timeout (30 - 255 sec, default = 90).	integer	Minimum value: 30 Maximum value: 255	90										

Parameter	Description	Type	Size	Default						
dial-cmd1	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63							
dial-cmd2	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63							
dial-cmd3	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63							
dial-on-demand	Enable/disable to dial the modem when packets are routed to the modem interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
distance	Distance of learned routes (1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255							
dont-send-CR1	Do not send CR when connected (ISP1).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dont-send-CR2	Do not send CR when connected (ISP2).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dont-send-CR3	Do not send CR when connected (ISP3).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
extra-init1	Extra initialization string to ISP 1.	string	Maximum length: 127							

Parameter	Description	Type	Size	Default								
extra-init2	Extra initialization string to ISP 2.	string	Maximum length: 127									
extra-init3	Extra initialization string to ISP 3.	string	Maximum length: 127									
holddown-timer	Hold down timer in seconds (1 - 60 sec).	integer	Minimum value: 1 Maximum value: 60	60								
idle-timer	MODEM connection idle time (1 - 9999 min, default = 5).	integer	Minimum value: 1 Maximum value: 9999	5								
interface	Name of redundant interface.	string	Maximum length: 63									
lockdown-lac	Allow connection only to the specified Location Area Code (LAC).	string	Maximum length: 127									
mode	Set MODEM operation mode to redundant or standalone.	option	-	standalone								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standalone</i></td><td>Standalone.</td></tr><tr><td><i>redundant</i></td><td>Redundant for an interface.</td></tr></table>				Option	Description	<i>standalone</i>	Standalone.	<i>redundant</i>	Redundant for an interface.		
Option	Description											
<i>standalone</i>	Standalone.											
<i>redundant</i>	Redundant for an interface.											
network-init	AT command to set the Network name/type (AT+COPS=<mode>,[<format>,<oper>[,<AcT>]]).	string	Maximum length: 127									
passwd1	Password to access the specified dialup account.	password	Not Specified									
passwd2	Password to access the specified dialup account.	password	Not Specified									
passwd3	Password to access the specified dialup account.	password	Not Specified									
peer-modem1	Specify peer MODEM type for phone1.	option	-	generic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>generic</i></td><td>All other modem type.</td></tr><tr><td><i>actiontec</i></td><td>ActionTec modem.</td></tr><tr><td><i>ascend_TNT</i></td><td>Ascend TNT modem.</td></tr></table>				Option	Description	<i>generic</i>	All other modem type.	<i>actiontec</i>	ActionTec modem.	<i>ascend_TNT</i>	Ascend TNT modem.
Option	Description											
<i>generic</i>	All other modem type.											
<i>actiontec</i>	ActionTec modem.											
<i>ascend_TNT</i>	Ascend TNT modem.											

Parameter	Description	Type	Size	Default								
peer-modem2	Specify peer MODEM type for phone2.	option	-	generic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>generic</i></td><td>All other modem type.</td></tr><tr><td><i>actiontec</i></td><td>ActionTec modem.</td></tr><tr><td><i>ascend_TNT</i></td><td>Ascend TNT modem.</td></tr></table>	Option	Description	<i>generic</i>	All other modem type.	<i>actiontec</i>	ActionTec modem.	<i>ascend_TNT</i>	Ascend TNT modem.			
Option	Description											
<i>generic</i>	All other modem type.											
<i>actiontec</i>	ActionTec modem.											
<i>ascend_TNT</i>	Ascend TNT modem.											
peer-modem3	Specify peer MODEM type for phone3.	option	-	generic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>generic</i></td><td>All other modem type.</td></tr><tr><td><i>actiontec</i></td><td>ActionTec modem.</td></tr><tr><td><i>ascend_TNT</i></td><td>Ascend TNT modem.</td></tr></table>	Option	Description	<i>generic</i>	All other modem type.	<i>actiontec</i>	ActionTec modem.	<i>ascend_TNT</i>	Ascend TNT modem.			
Option	Description											
<i>generic</i>	All other modem type.											
<i>actiontec</i>	ActionTec modem.											
<i>ascend_TNT</i>	Ascend TNT modem.											
phone1	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63									
phone2	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63									
phone3	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63									
pin-init	AT command to set the PIN (AT+PIN=<pin>).	string	Maximum length: 127									
ppp-echo-request1	Enable/disable PPP echo-request to ISP 1.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
ppp-echo-request2	Enable/disable PPP echo-request to ISP 2.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

Parameter	Description	Type	Size	Default
ppp-echo-request3	Enable/disable PPP echo-request to ISP 3.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
priority	Priority of learned routes (1 - 65535, default = 1).	integer	Minimum value: 1 Maximum value: 65535	1
redial	Redial limit (1 - 10 attempts, none = redial forever).	option	-	none
	Option	Description		
	<i>none</i>	Forever.		
	<i>1</i>	One attempt.		
	<i>2</i>	Two attempts.		
	<i>3</i>	Three attempts.		
	<i>4</i>	Four attempts.		
	<i>5</i>	Five attempts.		
	<i>6</i>	Six attempts.		
	<i>7</i>	Seven attempts.		
	<i>8</i>	Eight attempts.		
	<i>9</i>	Nine attempts.		
	<i>10</i>	Ten attempts.		
reset	Number of dial attempts before resetting modem (0 = never reset).	integer	Minimum value: 0 Maximum value: 10	0
status	Enable/disable Modem support (equivalent to bringing an interface up or down).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
traffic-check	Enable/disable traffic-check.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
username1	User name to access the specified dialup account.	string	Maximum length: 63	
username2	User name to access the specified dialup account.	string	Maximum length: 63	
username3	User name to access the specified dialup account.	string	Maximum length: 63	
wireless-port	Enter wireless port number: 0 for default, 1 for first port, and so on (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	

config system nd-proxy

Configure IPv6 neighbor discovery proxy (RFC4389).

```
config system nd-proxy
    Description: Configure IPv6 neighbor discovery proxy (RFC4389).
    set member <interface-name1>, <interface-name2>, ...
    set status [enable|disable]
end
```

config system nd-proxy

Parameter	Description	Type	Size	Default						
member <interface-name>	Interfaces using the neighbor discovery proxy. Interface name.	string	Maximum length: 79							
status	Enable/disable neighbor discovery proxy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable neighbor discovery proxy.</td></tr><tr><td><i>disable</i></td><td>Disable neighbor discovery proxy.</td></tr></table>				Option	Description	<i>enable</i>	Enable neighbor discovery proxy.	<i>disable</i>	Disable neighbor discovery proxy.
Option	Description									
<i>enable</i>	Enable neighbor discovery proxy.									
<i>disable</i>	Disable neighbor discovery proxy.									

config system netflow

Configure NetFlow.

```
config system netflow
  Description: Configure NetFlow.
  set active-flow-timeout {integer}
  config collectors
    Description: Netflow collectors.
    edit <id>
      set collector-ip {string}
      set collector-port {integer}
      set interface {string}
      set interface-select-method [auto|sdwan|...]
      set source-ip {string}
      set source-ip-interface {string}
      set vrf-select {integer}
    next
  end
  config exclusion-filters
    Description: Exclusion filters
    edit <id>
      set destination-ip {user}
      set destination-port {user}
      set protocol {integer}
      set source-ip {user}
      set source-port {user}
    next
  end
  set inactive-flow-timeout {integer}
  set session-cache-size [min|default|...]
  set template-tx-counter {integer}
  set template-tx-timeout {integer}
end
```

config system netflow

Parameter	Description	Type	Size	Default
active-flow-timeout	Timeout to report active flows (60 - 3600 sec, default = 1800).	integer	Minimum value: 60 Maximum value: 3600	1800
inactive-flow-timeout	Timeout for periodic report of finished flows (10 - 600 sec, default = 15).	integer	Minimum value: 10 Maximum value: 600	15

Parameter	Description	Type	Size	Default								
session-cache-size	Maximum RAM usage allowed for Netflow session cache.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>min</i></td><td>Up to 0.5% of system RAM.</td></tr><tr><td><i>default</i></td><td>Up to 1% of system RAM.</td></tr><tr><td><i>max</i></td><td>Up to 2% of system RAM.</td></tr></table>	Option	Description	<i>min</i>	Up to 0.5% of system RAM.	<i>default</i>	Up to 1% of system RAM.	<i>max</i>	Up to 2% of system RAM.			
Option	Description											
<i>min</i>	Up to 0.5% of system RAM.											
<i>default</i>	Up to 1% of system RAM.											
<i>max</i>	Up to 2% of system RAM.											
template-tx-counter	Counter of flowset records before resending a template flowset record.	integer	Minimum value: 10 Maximum value: 6000	20								
template-tx-timeout	Timeout for periodic template flowset transmission (60 - 86400 sec, default = 1800).	integer	Minimum value: 60 Maximum value: 86400	1800								

config collectors

Parameter	Description	Type	Size	Default				
collector-ip	Collector IP.	string	Maximum length: 63					
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535	2055				
id	ID.	integer	Minimum value: 1 Maximum value: 6	0				
interface	Specify outgoing interface to reach server.	string	Maximum length: 15					
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.
Option	Description							
auto	Set outgoing interface automatically.							

Parameter	Description	Type	Size	Default
	Option	Description		
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.		
	specify	Set outgoing interface manually.		
source-ip	Source IP address for communication with the NetFlow agent.	string	Maximum length: 63	
source-ip-interface	Name of the interface used to determine the source IP for exporting packets.	string	Maximum length: 15	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config exclusion-filters

Parameter	Description	Type	Size	Default
destination-ip	Session destination address.	user	Not Specified	
destination-port	Session destination port number or range.	user	Not Specified	
id	Filter ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Session IP protocol (0 - 255, default = 255, meaning any).	integer	Minimum value: 0 Maximum value: 255	255
source-ip	Session source address.	user	Not Specified	
source-port	Session source port number or range.	user	Not Specified	

config system network-visibility

Configure network visibility settings.

```

config system network-visibility
  Description: Configure network visibility settings.
  set destination-hostname-visibility [disable|enable]
  set destination-location [disable|enable]
  set destination-visibility [disable|enable]
  set source-location [disable|enable]
end

```

config system network-visibility

Parameter	Description	Type	Size	Default						
destination-hostname-visibility	Enable/disable logging of destination hostname visibility.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of destination hostname visibility.</td></tr><tr><td>enable</td><td>Enable logging of destination hostname visibility.</td></tr></table>	Option	Description	disable	Disable logging of destination hostname visibility.	enable	Enable logging of destination hostname visibility.			
Option	Description									
disable	Disable logging of destination hostname visibility.									
enable	Enable logging of destination hostname visibility.									
destination-location	Enable/disable logging of destination geographical location visibility.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of destination geographical location visibility.</td></tr><tr><td>enable</td><td>Enable logging of destination geographical location visibility.</td></tr></table>	Option	Description	disable	Disable logging of destination geographical location visibility.	enable	Enable logging of destination geographical location visibility.			
Option	Description									
disable	Disable logging of destination geographical location visibility.									
enable	Enable logging of destination geographical location visibility.									
destination-visibility	Enable/disable logging of destination visibility.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of destination visibility.</td></tr><tr><td>enable</td><td>Enable logging of destination visibility.</td></tr></table>	Option	Description	disable	Disable logging of destination visibility.	enable	Enable logging of destination visibility.			
Option	Description									
disable	Disable logging of destination visibility.									
enable	Enable logging of destination visibility.									
source-location	Enable/disable logging of source geographical location visibility.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of source geographical location visibility.</td></tr><tr><td>enable</td><td>Enable logging of source geographical location visibility.</td></tr></table>	Option	Description	disable	Disable logging of source geographical location visibility.	enable	Enable logging of source geographical location visibility.			
Option	Description									
disable	Disable logging of source geographical location visibility.									
enable	Enable logging of source geographical location visibility.									

config system ngfw-settings

Configure IPS NGFW policy-mode VDOM settings.

```
config system ngfw-settings
  Description: Configure IPS NGFW policy-mode VDOM settings.
  set match-timeout {integer}
  set tcp-halfopen-match-timeout {integer}
  set tcp-match-timeout {integer}
end
```

config system ngfw-settings

Parameter	Description	Type	Size	Default
match-timeout	Number of seconds to wait before a security policy match for an idle non-TCP session (0 - 1800, default = 300, 0 means unlimited).	integer	Minimum value: 0 Maximum value: 1800	300
tcp-halfopen-match-timeout	Number of seconds to wait before a security policy match for a session after one peer has sent an open session packet but the other has not responded (0 - 300, default = 8, 0 means unlimited).	integer	Minimum value: 0 Maximum value: 300	8
tcp-match-timeout	Number of seconds to wait before a security policy match for an idle TCP session (0 - 1800, default = 300, 0 means unlimited).	integer	Minimum value: 0 Maximum value: 1800	300

config system np6



This command is available for model(s): FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D.

It is not available for: FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 3200F, FortiGate 3201F, FortiGate 3500F, FortiGate 3501F, FortiGate 3700F, FortiGate 3701F, FortiGate 400F, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NP6 attributes.

```

config system np6
    Description: Configure NP6 attributes.
    edit <name>
        set fastpath [disable|enable]
        config fp-anomaly
            Description: NP6 IPv4 anomaly protection. trap-to-host forwards anomaly sessions to
the CPU.
            set icmp-csum-err [drop|trap-to-host]
            set icmp-frag [allow|drop|...]
            set icmp-land [allow|drop|...]
            set ipv4-csum-err [drop|trap-to-host]
            set ipv4-land [allow|drop|...]
            set ipv4-optlsrr [allow|drop|...]
            set ipv4-optrr [allow|drop|...]
            set ipv4-optsecurity [allow|drop|...]
            set ipv4-optssrr [allow|drop|...]
            set ipv4-optstream [allow|drop|...]
            set ipv4-opttimestamp [allow|drop|...]
            set ipv4-proto-err [allow|drop|...]
            set ipv4-unknopt [allow|drop|...]
            set ipv6-daddr-err [allow|drop|...]
            set ipv6-land [allow|drop|...]
            set ipv6-optendpid [allow|drop|...]
            set ipv6-opthomeaddr [allow|drop|...]
            set ipv6-optinvld [allow|drop|...]
            set ipv6-optjumbo [allow|drop|...]
            set ipv6-optnsap [allow|drop|...]
            set ipv6-optralert [allow|drop|...]
            set ipv6-opttunnel [allow|drop|...]
            set ipv6-proto-err [allow|drop|...]
            set ipv6-saddr-err [allow|drop|...]
            set ipv6-unknopt [allow|drop|...]
            set tcp-csum-err [drop|trap-to-host]
            set tcp-fin-noack [allow|drop|...]
            set tcp-fin-only [allow|drop|...]
            set tcp-land [allow|drop|...]
            set tcp-no-flag [allow|drop|...]
            set tcp-syn-data [allow|drop|...]
            set tcp-syn-fin [allow|drop|...]
            set tcp-winnuke [allow|drop|...]
            set udp-csum-err [drop|trap-to-host]
            set udp-land [allow|drop|...]
        end
    set garbage-session-collector [disable|enable]
    config hpe
        Description: HPE configuration.
        set arp-max {integer}
        set enable-shaper [disable|enable]
        set esp-max {integer}
        set icmp-max {integer}
        set ip-frag-max {integer}
        set ip-others-max {integer}

```

```

        set l2-others-max {integer}
        set pri-type-max {integer}
        set sctp-max {integer}
        set tcp-max {integer}
        set tcpfin-rst-max {integer}
        set tcpsyn-ack-max {integer}
        set tcpsyn-max {integer}
        set udp-max {integer}
    end
    set ipsec-ob-hash-function [switch-group-hash|global-hash|...]
    set ipsec-outbound-hash [disable|enable]
    set low-latency-mode [disable|enable]
    set per-session-accounting [disable|traffic-log-only|...]
    set session-collector-interval {integer}
    set session-timeout-fixed [disable|enable]
    set session-timeout-interval {integer}
    set session-timeout-random-range {integer}
next
end

```

config system np6

Parameter	Description	Type	Size	Default
fastpath	Enable/disable NP6 offloading (also called fast path).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable NP6 offloading (fast path).		
	<i>enable</i>	Enable NP6 offloading (fast path).		
garbage-session-collector	Enable/disable garbage session collector.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable garbage session collector.		
	<i>enable</i>	Enable garbage session collector.		
ipsec-ob-hash-function *	Set hash function for IPSec outbound.	option	-	switch-group-hash

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>switch-group-hash</i>	Hash outbound SA traffic within NPs connected to same switch.		
	<i>global-hash</i>	Hash outbound SA traffic among all NPs.		
	<i>global-hash-weighted</i>	Hash outbound SA traffic among all NPs with more weights on NPs connected to switch 0. It's applicable to the case that ingress traffic is from switch 1.		
	<i>round-robin-switch-group</i>	Round-robin outbound SA traffic within NPs connected to same switch.		
	<i>round-robin-global</i>	Round-robin outbound SA traffic among all NPs.		
ipsec-outbound-hash *	Enable/disable hash function for IPsec outbound traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable hash function for IPsec outbound traffic.		
	<i>enable</i>	Enable hash function for IPsec outbound traffic.		
low-latency-mode	Enable/disable low latency mode.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable low latency mode.		
	<i>enable</i>	Enable low latency mode.		
name	Device Name.	string	Maximum length: 31	
per-session-accounting	Enable/disable per-session accounting.	option	-	traffic-log-only
	Option	Description		
	<i>disable</i>	Disable per-session accounting.		
	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enabled in firewall policy.		
	<i>enable</i>	Per-session accounting for all sessions.		

Parameter	Description	Type	Size	Default						
session-collector-interval	Set garbage session collection cleanup interval (1 - 100 sec, default 64).	integer	Minimum value: 1 Maximum value: 100	64						
session-timeout-fixed	{disable enable} Toggle between using fixed or random timeouts for refreshing NP6 sessions.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Refresh NP6 sessions at the configured fixed interval.</td></tr><tr><td>enable</td><td>Enable Refresh NP6 sessions randomly where the time between refreshes is within the random range.</td></tr></table>				Option	Description	disable	Disable Refresh NP6 sessions at the configured fixed interval.	enable	Enable Refresh NP6 sessions randomly where the time between refreshes is within the random range.
Option	Description									
disable	Disable Refresh NP6 sessions at the configured fixed interval.									
enable	Enable Refresh NP6 sessions randomly where the time between refreshes is within the random range.									
session-timeout-interval	Set the fixed timeout for refreshing NP6 sessions (0 - 1000 sec, default 40 sec).	integer	Minimum value: 0 Maximum value: 1000	40						
session-timeout-random-range	Set the random timeout range for refreshing NP6 sessions (0 - 1000 sec, default 8 sec).	integer	Minimum value: 0 Maximum value: 1000	8						

* This parameter may not exist in some models.

config fp-anomaly

Parameter	Description	Type	Size	Default								
icmp-csum-err	Invalid IPv4 ICMP checksum anomalies.	option	-	drop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid ICMP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid ICMP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid ICMP checksum.	trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.					
Option	Description											
drop	Drop IPv4 invalid ICMP checksum.											
trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.											
icmp-frag	Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow L3 fragment packet with L4 protocol as ICMP attack to pass.</td></tr><tr><td>drop</td><td>Drop L3 fragment packet with L4 protocol as ICMP attack.</td></tr><tr><td>trap-to-host</td><td>Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.	drop	Drop L3 fragment packet with L4 protocol as ICMP attack.	trap-to-host	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.			
Option	Description											
allow	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.											
drop	Drop L3 fragment packet with L4 protocol as ICMP attack.											
trap-to-host	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.											

Parameter	Description	Type	Size	Default								
icmp-land	ICMP land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow ICMP land attack to pass.</td></tr><tr><td>drop</td><td>Drop ICMP land attack.</td></tr><tr><td>trap-to-host</td><td>Forward ICMP land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow ICMP land attack to pass.	drop	Drop ICMP land attack.	trap-to-host	Forward ICMP land attack to FortiOS.			
Option	Description											
allow	Allow ICMP land attack to pass.											
drop	Drop ICMP land attack.											
trap-to-host	Forward ICMP land attack to FortiOS.											
ipv4-csum-err	Invalid IPv4 IP checksum anomalies.	option	-	drop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid IP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid IP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid IP checksum.	trap-to-host	Forward IPv4 invalid IP checksum to main CPU for processing.					
Option	Description											
drop	Drop IPv4 invalid IP checksum.											
trap-to-host	Forward IPv4 invalid IP checksum to main CPU for processing.											
ipv4-land	Land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 land attack to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 land attack.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 land attack to pass.	drop	Drop IPv4 land attack.	trap-to-host	Forward IPv4 land attack to FortiOS.			
Option	Description											
allow	Allow IPv4 land attack to pass.											
drop	Drop IPv4 land attack.											
trap-to-host	Forward IPv4 land attack to FortiOS.											
ipv4-optlrr	Loose source record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with loose source record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with loose source record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with loose source record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with loose source record route option to pass.	drop	Drop IPv4 with loose source record route option.	trap-to-host	Forward IPv4 with loose source record route option to FortiOS.			
Option	Description											
allow	Allow IPv4 with loose source record route option to pass.											
drop	Drop IPv4 with loose source record route option.											
trap-to-host	Forward IPv4 with loose source record route option to FortiOS.											
ipv4-optrr	Record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with record route option to pass.	drop	Drop IPv4 with record route option.	trap-to-host	Forward IPv4 with record route option to FortiOS.			
Option	Description											
allow	Allow IPv4 with record route option to pass.											
drop	Drop IPv4 with record route option.											
trap-to-host	Forward IPv4 with record route option to FortiOS.											
ipv4-optsecurity	Security option anomalies.	option	-	trap-to-host								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>allow</i>	Allow IPv4 with security option to pass.		
	<i>drop</i>	Drop IPv4 with security option.		
	<i>trap-to-host</i>	Forward IPv4 with security option to FortiOS.		
ipv4-optssrr	Strict source record route option anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow IPv4 with strict source record route option to pass.		
	<i>drop</i>	Drop IPv4 with strict source record route option.		
	<i>trap-to-host</i>	Forward IPv4 with strict source record route option to FortiOS.		
ipv4-optstream	Stream option anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow IPv4 with stream option to pass.		
	<i>drop</i>	Drop IPv4 with stream option.		
	<i>trap-to-host</i>	Forward IPv4 with stream option to FortiOS.		
ipv4-opttimestamp	Timestamp option anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow IPv4 with timestamp option to pass.		
	<i>drop</i>	Drop IPv4 with timestamp option.		
	<i>trap-to-host</i>	Forward IPv4 with timestamp option to FortiOS.		
ipv4-proto-err	Invalid layer 4 protocol anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow IPv4 invalid L4 protocol to pass.		
	<i>drop</i>	Drop IPv4 invalid L4 protocol.		
	<i>trap-to-host</i>	Forward IPv4 invalid L4 protocol to FortiOS.		
ipv4-unknpt	Unknown option anomalies.	option	-	trap-to-host

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv4 with unknown options to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv4 with unknown options.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv4 with unknown options to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv4 with unknown options to pass.	<i>drop</i>	Drop IPv4 with unknown options.	<i>trap-to-host</i>	Forward IPv4 with unknown options to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv4 with unknown options to pass.										
	<i>drop</i>	Drop IPv4 with unknown options.										
<i>trap-to-host</i>	Forward IPv4 with unknown options to FortiOS.											
ipv6-daddr-err	Destination address as unspecified or loopback address anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with destination address as unspecified or loopback address to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with destination address as unspecified or loopback address.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with destination address as unspecified or loopback address to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with destination address as unspecified or loopback address to pass.	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.	<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 with destination address as unspecified or loopback address to pass.										
	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.										
<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.											
ipv6-land	Land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 land attack to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 land attack.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 land attack to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 land attack to pass.	<i>drop</i>	Drop IPv6 land attack.	<i>trap-to-host</i>	Forward IPv6 land attack to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 land attack to pass.										
	<i>drop</i>	Drop IPv6 land attack.										
<i>trap-to-host</i>	Forward IPv6 land attack to FortiOS.											
ipv6-optendpid	End point identification anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with end point identification option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with end point identification option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with end point identification option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with end point identification option to pass.	<i>drop</i>	Drop IPv6 with end point identification option.	<i>trap-to-host</i>	Forward IPv6 with end point identification option to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 with end point identification option to pass.										
	<i>drop</i>	Drop IPv6 with end point identification option.										
<i>trap-to-host</i>	Forward IPv6 with end point identification option to FortiOS.											
ipv6-opthomeaddr	Home address option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with home address option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with home address option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with home address option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with home address option to pass.	<i>drop</i>	Drop IPv6 with home address option.	<i>trap-to-host</i>	Forward IPv6 with home address option to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 with home address option to pass.										
	<i>drop</i>	Drop IPv6 with home address option.										
<i>trap-to-host</i>	Forward IPv6 with home address option to FortiOS.											

Parameter	Description	Type	Size	Default								
ipv6-optinvld	Invalid option anomalies.Invalid option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with invalid option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with invalid option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with invalid option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with invalid option to pass.	<i>drop</i>	Drop IPv6 with invalid option.	<i>trap-to-host</i>	Forward IPv6 with invalid option to FortiOS.			
Option	Description											
<i>allow</i>	Allow IPv6 with invalid option to pass.											
<i>drop</i>	Drop IPv6 with invalid option.											
<i>trap-to-host</i>	Forward IPv6 with invalid option to FortiOS.											
ipv6-optjumbo	Jumbo options anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with jumbo option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with jumbo option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with jumbo option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with jumbo option to pass.	<i>drop</i>	Drop IPv6 with jumbo option.	<i>trap-to-host</i>	Forward IPv6 with jumbo option to FortiOS.			
Option	Description											
<i>allow</i>	Allow IPv6 with jumbo option to pass.											
<i>drop</i>	Drop IPv6 with jumbo option.											
<i>trap-to-host</i>	Forward IPv6 with jumbo option to FortiOS.											
ipv6-optnsap	Network service access point address option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with network service access point address option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with network service access point address option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with network service access point address option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with network service access point address option to pass.	<i>drop</i>	Drop IPv6 with network service access point address option.	<i>trap-to-host</i>	Forward IPv6 with network service access point address option to FortiOS.			
Option	Description											
<i>allow</i>	Allow IPv6 with network service access point address option to pass.											
<i>drop</i>	Drop IPv6 with network service access point address option.											
<i>trap-to-host</i>	Forward IPv6 with network service access point address option to FortiOS.											
ipv6-optralert	Router alert option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with router alert option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with router alert option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with router alert option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with router alert option to pass.	<i>drop</i>	Drop IPv6 with router alert option.	<i>trap-to-host</i>	Forward IPv6 with router alert option to FortiOS.			
Option	Description											
<i>allow</i>	Allow IPv6 with router alert option to pass.											
<i>drop</i>	Drop IPv6 with router alert option.											
<i>trap-to-host</i>	Forward IPv6 with router alert option to FortiOS.											
ipv6-opttunnel	Tunnel encapsulation limit option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with tunnel encapsulation limit to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with tunnel encapsulation limit.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with tunnel encapsulation limit to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with tunnel encapsulation limit to pass.	<i>drop</i>	Drop IPv6 with tunnel encapsulation limit.	<i>trap-to-host</i>	Forward IPv6 with tunnel encapsulation limit to FortiOS.			
Option	Description											
<i>allow</i>	Allow IPv6 with tunnel encapsulation limit to pass.											
<i>drop</i>	Drop IPv6 with tunnel encapsulation limit.											
<i>trap-to-host</i>	Forward IPv6 with tunnel encapsulation limit to FortiOS.											

Parameter	Description	Type	Size	Default								
ipv6-proto-err	Layer 4 invalid protocol anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 L4 invalid protocol to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 L4 invalid protocol.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 L4 invalid protocol to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 L4 invalid protocol to pass.	drop	Drop IPv6 L4 invalid protocol.	trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.			
	Option	Description										
	allow	Allow IPv6 L4 invalid protocol to pass.										
	drop	Drop IPv6 L4 invalid protocol.										
trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.											
ipv6-saddr-err	Source address as multicast anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with source address as multicast to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with source address as multicast.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with source address as multicast to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with source address as multicast to pass.	drop	Drop IPv6 with source address as multicast.	trap-to-host	Forward IPv6 with source address as multicast to FortiOS.			
	Option	Description										
	allow	Allow IPv6 with source address as multicast to pass.										
	drop	Drop IPv6 with source address as multicast.										
trap-to-host	Forward IPv6 with source address as multicast to FortiOS.											
ipv6-unknpt	Unknown option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with unknown options to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with unknown options.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with unknown options to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with unknown options to pass.	drop	Drop IPv6 with unknown options.	trap-to-host	Forward IPv6 with unknown options to FortiOS.			
	Option	Description										
	allow	Allow IPv6 with unknown options to pass.										
	drop	Drop IPv6 with unknown options.										
trap-to-host	Forward IPv6 with unknown options to FortiOS.											
tcp-csum-err	Invalid IPv4 TCP checksum anomalies.	option	-	drop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid TCP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid TCP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid TCP checksum.	trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.					
	Option	Description										
	drop	Drop IPv4 invalid TCP checksum.										
trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.											
tcp-fin-noack	TCP SYN flood with FIN flag set without ACK setting anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow TCP packets with FIN flag set without ack setting to pass.</td></tr><tr><td>drop</td><td>Drop TCP packets with FIN flag set without ack setting.</td></tr><tr><td>trap-to-host</td><td>Forward TCP packets with FIN flag set without ack setting to FortiOS.</td></tr></table>	Option	Description	allow	Allow TCP packets with FIN flag set without ack setting to pass.	drop	Drop TCP packets with FIN flag set without ack setting.	trap-to-host	Forward TCP packets with FIN flag set without ack setting to FortiOS.			
	Option	Description										
	allow	Allow TCP packets with FIN flag set without ack setting to pass.										
	drop	Drop TCP packets with FIN flag set without ack setting.										
trap-to-host	Forward TCP packets with FIN flag set without ack setting to FortiOS.											
tcp-fin-only	TCP SYN flood with only FIN flag set anomalies.	option	-	trap-to-host								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>allow</i>	Allow TCP packets with FIN flag set only to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set only.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set only to FortiOS.		
tcp-land	TCP land anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow TCP land attack to pass.		
	<i>drop</i>	Drop TCP land attack.		
	<i>trap-to-host</i>	Forward TCP land attack to FortiOS.		
tcp-no-flag	TCP SYN flood with no flag set anomalies.	option	-	allow
	Option Description			
	<i>allow</i>	Allow TCP packets without flag set to pass.		
	<i>drop</i>	Drop TCP packets without flag set.		
	<i>trap-to-host</i>	Forward TCP packets without flag set to FortiOS.		
tcp-syn-data	TCP SYN flood packets with data anomalies.	option	-	allow
	Option Description			
	<i>allow</i>	Allow TCP syn packets with data to pass.		
	<i>drop</i>	Drop TCP syn packets with data.		
	<i>trap-to-host</i>	Forward TCP syn packets with data to FortiOS.		
tcp-syn-fin	TCP SYN flood SYN/FIN flag set anomalies.	option	-	allow
	Option Description			
	<i>allow</i>	Allow TCP packets with syn_fin flag set to pass.		
	<i>drop</i>	Drop TCP packets with syn_fin flag set.		
	<i>trap-to-host</i>	Forward TCP packets with syn_fin flag set to FortiOS.		
tcp-winnuke	TCP WinNuke anomalies.	option	-	trap-to-host

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow TCP packets winnuker attack to pass.		
	<i>drop</i>	Drop TCP packets winnuker attack.		
	<i>trap-to-host</i>	Forward TCP packets winnuker attack to FortiOS.		
udp-csum-err	Invalid IPv4 UDP checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP checksum to main CPU for processing.		
udp-land	UDP land anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow UDP land attack to pass.		
	<i>drop</i>	Drop UDP land attack.		
	<i>trap-to-host</i>	Forward UDP land attack to FortiOS.		

config hpe

Parameter	Description	Type	Size	Default
arp-max	Maximum ARP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
enable-shaper	Enable/Disable NPU Host Protection Engine (HPE) for packet type shaper.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable NPU HPE shaping based on packet type.		
	<i>enable</i>	Enable NPU HPE shaping based on packet type.		
esp-max	Maximum ESP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000

Parameter	Description	Type	Size	Default
icmp-max	Maximum ICMP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
ip-frag-max	Maximum fragmented IP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
ip-others-max	Maximum IP packet rate for other packets (packet types that cannot be set with other options) (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
l2-others-max	Maximum L2 packet rate for L2 packets that are not ARP packets (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
pri-type-max	Maximum overflow rate of priority type traffic (1K - 1G pps, default = 200K pps). Includes L2: HA, 802.3ad LACP, heartbeats. L3: OSPF. L4: TCP: BGP. L4_UDP: IKE, SLBC, BFD.	integer	Minimum value: 1000 Maximum value: 1000000000	200000
sctp-max	Maximum SCTP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
tcp-max	Maximum TCP packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	600000
tcpfin-rst-max	Maximum TCP carries FIN or RST flags packet rate (1K - 1G pps, default = 60K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	600000

Parameter	Description	Type	Size	Default
tcpsyn-ack-max	Maximum TCP carries SYN and ACK flags packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	600000
tcpsyn-max	Maximum TCP SYN packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	600000
udp-max	Maximum UDP packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	600000

config system np6xlite



This command is available for model(s): FortiGate 100F, FortiGate 101F, FortiGate 200F, FortiGate 201F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 800D, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

Configure NP6XLITE attributes.

```

config system np6xlite
    Description: Configure NP6XLITE attributes.
    edit <name>
        set congestion-handling-mode [flow-control|head-of-line]
        set fastpath [disable|enable]
        config fp-anomaly
            Description: NP6XLITE IPv4 anomaly protection. The trap-to-host forwards anomaly
sessions to the CPU.
            set icmp-csum-err [drop|trap-to-host]
            set icmp-frag [allow|drop|...]
            set icmp-land [allow|drop|...]
            set ipv4-csum-err [drop|trap-to-host]
            set ipv4-land [allow|drop|...]
            set ipv4-optlsrr [allow|drop|...]
            set ipv4-optrr [allow|drop|...]
            set ipv4-optsecurity [allow|drop|...]
            set ipv4-optssrr [allow|drop|...]
            set ipv4-optstream [allow|drop|...]
            set ipv4-opttimestamp [allow|drop|...]
            set ipv4-proto-err [allow|drop|...]
            set ipv4-unknopt [allow|drop|...]
            set ipv6-daddr-err [allow|drop|...]
            set ipv6-land [allow|drop|...]
            set ipv6-optendpid [allow|drop|...]
            set ipv6-opthomeaddr [allow|drop|...]
            set ipv6-optinvld [allow|drop|...]
            set ipv6-optjumbo [allow|drop|...]
            set ipv6-optnsap [allow|drop|...]
            set ipv6-optralert [allow|drop|...]
            set ipv6-opttunnel [allow|drop|...]
            set ipv6-proto-err [allow|drop|...]
            set ipv6-saddr-err [allow|drop|...]
            set ipv6-unknopt [allow|drop|...]
            set tcp-csum-err [drop|trap-to-host]
            set tcp-fin-noack [allow|drop|...]
            set tcp-fin-only [allow|drop|...]
            set tcp-land [allow|drop|...]
            set tcp-no-flag [allow|drop|...]
            set tcp-syn-data [allow|drop|...]
            set tcp-syn-fin [allow|drop|...]
            set tcp-winnuke [allow|drop|...]
            set udp-csum-err [drop|trap-to-host]
            set udp-land [allow|drop|...]
        end
    config hpe
        Description: HPE configuration.
        set arp-max {integer}
        set enable-shaper [disable|enable]
        set esp-max {integer}
        set icmp-max {integer}
        set ip-frag-max {integer}
        set ip-others-max {integer}

```

```

        set l2-others-max {integer}
        set pri-type-max {integer}
        set sctp-max {integer}
        set tcp-others-max {integer}
        set tcpfin-rst-max {integer}
        set tcpsyn-ack-max {integer}
        set tcpsyn-max {integer}
        set udp-max {integer}
    end
    set ipsec-inner-fragment [disable|enable]
    set ipsec-sts-timeout [1|2|...]
    set ipsec-throughput-msg-frequency [disable|32kb|...]
    set per-session-accounting [disable|traffic-log-only|...]
    set session-timeout-interval {integer}
next
end

```

config system np6xlite

Parameter	Description	Type	Size	Default						
congestion-handling-mode *	Configure Marvell switch packet congestion handling.	option	-	head-of-line						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>flow-control</td><td>Pause peer sending additional traffic until congestion is resolved.</td></tr><tr><td>head-of-line</td><td>Drop excessive traffic until congestion is resolved.</td></tr></table>	Option	Description	flow-control	Pause peer sending additional traffic until congestion is resolved.	head-of-line	Drop excessive traffic until congestion is resolved.			
Option	Description									
flow-control	Pause peer sending additional traffic until congestion is resolved.									
head-of-line	Drop excessive traffic until congestion is resolved.									
fastpath	Enable/disable NP6XLITE offloading (also called fast path).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NP6XLITE offloading (fast path).</td></tr><tr><td>enable</td><td>Enable NP6XLITE offloading (fast path).</td></tr></table>	Option	Description	disable	Disable NP6XLITE offloading (fast path).	enable	Enable NP6XLITE offloading (fast path).			
Option	Description									
disable	Disable NP6XLITE offloading (fast path).									
enable	Enable NP6XLITE offloading (fast path).									
ipsec-inner-fragment	Enable/disable NP6XLite IPsec fragmentation type: inner.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>NP6XLite ipsec fragmentation type: outer.</td></tr><tr><td>enable</td><td>Enable NP6XLite ipsec fragmentation type: inner.</td></tr></table>	Option	Description	disable	NP6XLite ipsec fragmentation type: outer.	enable	Enable NP6XLite ipsec fragmentation type: inner.			
Option	Description									
disable	NP6XLite ipsec fragmentation type: outer.									
enable	Enable NP6XLite ipsec fragmentation type: inner.									
ipsec-sts-timeout	Set NP6XLite IPsec STS message timeout.	option	-	5						

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Set NP6Xlite STS message timeout to 1 sec (recommended for IPSec throughput GUI).</td></tr><tr><td>2</td><td>Set NP6Xlite STS message timeout to 2 sec.</td></tr><tr><td>3</td><td>Set NP6Xlite STS message timeout to 3 sec.</td></tr><tr><td>4</td><td>Set NP6Xlite STS message timeout to 4 sec.</td></tr><tr><td>5</td><td>Set NP6Xlite STS message timeout to 5 sec (default).</td></tr><tr><td>6</td><td>Set NP6Xlite STS message timeout to 6 sec.</td></tr><tr><td>7</td><td>Set NP6Xlite STS message timeout to 7 sec.</td></tr><tr><td>8</td><td>Set NP6Xlite STS message timeout to 8 sec.</td></tr><tr><td>9</td><td>Set NP6Xlite STS message timeout to 9 sec.</td></tr><tr><td>10</td><td>Set NP6Xlite STS message timeout to 10 sec.</td></tr></table>	Option	Description	1	Set NP6Xlite STS message timeout to 1 sec (recommended for IPSec throughput GUI).	2	Set NP6Xlite STS message timeout to 2 sec.	3	Set NP6Xlite STS message timeout to 3 sec.	4	Set NP6Xlite STS message timeout to 4 sec.	5	Set NP6Xlite STS message timeout to 5 sec (default).	6	Set NP6Xlite STS message timeout to 6 sec.	7	Set NP6Xlite STS message timeout to 7 sec.	8	Set NP6Xlite STS message timeout to 8 sec.	9	Set NP6Xlite STS message timeout to 9 sec.	10	Set NP6Xlite STS message timeout to 10 sec.									
	Option	Description																														
	1	Set NP6Xlite STS message timeout to 1 sec (recommended for IPSec throughput GUI).																														
	2	Set NP6Xlite STS message timeout to 2 sec.																														
	3	Set NP6Xlite STS message timeout to 3 sec.																														
	4	Set NP6Xlite STS message timeout to 4 sec.																														
	5	Set NP6Xlite STS message timeout to 5 sec (default).																														
	6	Set NP6Xlite STS message timeout to 6 sec.																														
	7	Set NP6Xlite STS message timeout to 7 sec.																														
	8	Set NP6Xlite STS message timeout to 8 sec.																														
	9	Set NP6Xlite STS message timeout to 9 sec.																														
10	Set NP6Xlite STS message timeout to 10 sec.																															
ipsec-throughput-msg-frequency	Set NP6XLite IPsec throughput message frequency (0 = disable).	option	-	disable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NP6Xlite throughput update message.</td></tr><tr><td>32kb</td><td>Set NP6Xlite throughput update message frequency to 32KB.</td></tr><tr><td>64kb</td><td>Set NP6Xlite throughput update message frequency to 64KB.</td></tr><tr><td>128kb</td><td>Set NP6Xlite throughput update message frequency to 128KB.</td></tr><tr><td>256kb</td><td>Set NP6Xlite throughput update message frequency to 256KB.</td></tr><tr><td>512kb</td><td>Set NP6Xlite throughput update message frequency to 512KB.</td></tr><tr><td>1mb</td><td>Set NP6Xlite throughput update message frequency to 1MB.</td></tr><tr><td>2mb</td><td>Set NP6Xlite throughput update message frequency to 2MB.</td></tr><tr><td>4mb</td><td>Set NP6Xlite throughput update message frequency to 4MB.</td></tr><tr><td>8mb</td><td>Set NP6Xlite throughput update message frequency to 8MB.</td></tr><tr><td>16mb</td><td>Set NP6Xlite throughput update message frequency to 16MB.</td></tr><tr><td>32mb</td><td>Set NP6Xlite throughput update message frequency to 32MB.</td></tr><tr><td>64mb</td><td>Set NP6Xlite throughput update message frequency to 64MB.</td></tr></table>	Option	Description	disable	Disable NP6Xlite throughput update message.	32kb	Set NP6Xlite throughput update message frequency to 32KB.	64kb	Set NP6Xlite throughput update message frequency to 64KB.	128kb	Set NP6Xlite throughput update message frequency to 128KB.	256kb	Set NP6Xlite throughput update message frequency to 256KB.	512kb	Set NP6Xlite throughput update message frequency to 512KB.	1mb	Set NP6Xlite throughput update message frequency to 1MB.	2mb	Set NP6Xlite throughput update message frequency to 2MB.	4mb	Set NP6Xlite throughput update message frequency to 4MB.	8mb	Set NP6Xlite throughput update message frequency to 8MB.	16mb	Set NP6Xlite throughput update message frequency to 16MB.	32mb	Set NP6Xlite throughput update message frequency to 32MB.	64mb	Set NP6Xlite throughput update message frequency to 64MB.			
	Option	Description																														
	disable	Disable NP6Xlite throughput update message.																														
	32kb	Set NP6Xlite throughput update message frequency to 32KB.																														
	64kb	Set NP6Xlite throughput update message frequency to 64KB.																														
	128kb	Set NP6Xlite throughput update message frequency to 128KB.																														
	256kb	Set NP6Xlite throughput update message frequency to 256KB.																														
	512kb	Set NP6Xlite throughput update message frequency to 512KB.																														
	1mb	Set NP6Xlite throughput update message frequency to 1MB.																														
	2mb	Set NP6Xlite throughput update message frequency to 2MB.																														
	4mb	Set NP6Xlite throughput update message frequency to 4MB.																														
	8mb	Set NP6Xlite throughput update message frequency to 8MB.																														
	16mb	Set NP6Xlite throughput update message frequency to 16MB.																														
	32mb	Set NP6Xlite throughput update message frequency to 32MB.																														
	64mb	Set NP6Xlite throughput update message frequency to 64MB.																														

Parameter	Description	Type	Size	Default
	Option	Description		
	128mb	Set NP6Xlite throughput update message frequency to 128MB.		
	256mb	Set NP6Xlite throughput update message frequency to 256MB.		
	512mb	Set NP6Xlite throughput update message frequency to 512MB.		
	1gb	Set NP6Xlite throughput update message frequency to 1GB.		
name	Device Name.	string	Maximum length: 31	
per-session-accounting	Enable/disable per-session accounting.	option	-	traffic-log-only
	Option	Description		
	disable	Disable per-session accounting.		
	traffic-log-only	Per-session accounting only for sessions with traffic logging enabled in firewall policy.		
	enable	Per-session accounting for all sessions.		
session-timeout-interval	Set session timeout interval (0 - 1000 sec, default 40 sec).	integer	Minimum value: 0 Maximum value: 1000	40

* This parameter may not exist in some models.

config fp-anomaly

Parameter	Description	Type	Size	Default						
icmp-csum-err	Invalid IPv4 ICMP checksum anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>drop</i></td><td>Drop IPv4 invalid ICMP checksum.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv4 invalid ICMP checksum to main CPU for processing.</td></tr></table>	Option	Description	<i>drop</i>	Drop IPv4 invalid ICMP checksum.	<i>trap-to-host</i>	Forward IPv4 invalid ICMP checksum to main CPU for processing.			
Option	Description									
<i>drop</i>	Drop IPv4 invalid ICMP checksum.									
<i>trap-to-host</i>	Forward IPv4 invalid ICMP checksum to main CPU for processing.									
icmp-frag	Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow L3 fragment packet with L4 protocol as ICMP attack to pass.</td></tr><tr><td><i>drop</i></td><td>Drop L3 fragment packet with L4 protocol as ICMP attack.</td></tr></table>	Option	Description	<i>allow</i>	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.	<i>drop</i>	Drop L3 fragment packet with L4 protocol as ICMP attack.			
Option	Description									
<i>allow</i>	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.									
<i>drop</i>	Drop L3 fragment packet with L4 protocol as ICMP attack.									

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>trap-to-host</i></td><td>Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.</td></tr></table>	Option	Description	<i>trap-to-host</i>	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.							
	Option	Description										
<i>trap-to-host</i>	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.											
icmp-land	ICMP land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow ICMP land attack to pass.</td></tr><tr><td><i>drop</i></td><td>Drop ICMP land attack.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward ICMP land attack to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow ICMP land attack to pass.	<i>drop</i>	Drop ICMP land attack.	<i>trap-to-host</i>	Forward ICMP land attack to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow ICMP land attack to pass.										
	<i>drop</i>	Drop ICMP land attack.										
<i>trap-to-host</i>	Forward ICMP land attack to FortiOS.											
ipv4-csum-err	Invalid IPv4 IP checksum anomalies.	option	-	drop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>drop</i></td><td>Drop IPv4 invalid IP checksum.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv4 invalid IP checksum to main CPU for processing.</td></tr></table>	Option	Description	<i>drop</i>	Drop IPv4 invalid IP checksum.	<i>trap-to-host</i>	Forward IPv4 invalid IP checksum to main CPU for processing.					
	Option	Description										
	<i>drop</i>	Drop IPv4 invalid IP checksum.										
<i>trap-to-host</i>	Forward IPv4 invalid IP checksum to main CPU for processing.											
ipv4-land	Land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv4 land attack to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv4 land attack.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv4 land attack to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv4 land attack to pass.	<i>drop</i>	Drop IPv4 land attack.	<i>trap-to-host</i>	Forward IPv4 land attack to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv4 land attack to pass.										
	<i>drop</i>	Drop IPv4 land attack.										
<i>trap-to-host</i>	Forward IPv4 land attack to FortiOS.											
ipv4-optlrr	Loose source record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv4 with loose source record route option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv4 with loose source record route option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv4 with loose source record route option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv4 with loose source record route option to pass.	<i>drop</i>	Drop IPv4 with loose source record route option.	<i>trap-to-host</i>	Forward IPv4 with loose source record route option to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv4 with loose source record route option to pass.										
	<i>drop</i>	Drop IPv4 with loose source record route option.										
<i>trap-to-host</i>	Forward IPv4 with loose source record route option to FortiOS.											
ipv4-optrr	Record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv4 with record route option to pass.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv4 with record route option to pass.							
	Option	Description										
<i>allow</i>	Allow IPv4 with record route option to pass.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>drop</i>	Drop IPv4 with record route option.		
	<i>trap-to-host</i>	Forward IPv4 with record route option to FortiOS.		
ipv4-optsecurity	Security option anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow IPv4 with security option to pass.		
	<i>drop</i>	Drop IPv4 with security option.		
	<i>trap-to-host</i>	Forward IPv4 with security option to FortiOS.		
ipv4-optssrr	Strict source record route option anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow IPv4 with strict source record route option to pass.		
	<i>drop</i>	Drop IPv4 with strict source record route option.		
	<i>trap-to-host</i>	Forward IPv4 with strict source record route option to FortiOS.		
ipv4-optstream	Stream option anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow IPv4 with stream option to pass.		
	<i>drop</i>	Drop IPv4 with stream option.		
	<i>trap-to-host</i>	Forward IPv4 with stream option to FortiOS.		
ipv4-opttimestamp	Timestamp option anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow IPv4 with timestamp option to pass.		
	<i>drop</i>	Drop IPv4 with timestamp option.		
	<i>trap-to-host</i>	Forward IPv4 with timestamp option to FortiOS.		
ipv4-proto-err	Invalid layer 4 protocol anomalies.	option	-	trap-to-host

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv4 invalid L4 protocol to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv4 invalid L4 protocol.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv4 invalid L4 protocol to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv4 invalid L4 protocol to pass.	<i>drop</i>	Drop IPv4 invalid L4 protocol.	<i>trap-to-host</i>	Forward IPv4 invalid L4 protocol to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv4 invalid L4 protocol to pass.										
	<i>drop</i>	Drop IPv4 invalid L4 protocol.										
<i>trap-to-host</i>	Forward IPv4 invalid L4 protocol to FortiOS.											
ipv4-unknopt	Unknown option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv4 with unknown options to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv4 with unknown options.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv4 with unknown options to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv4 with unknown options to pass.	<i>drop</i>	Drop IPv4 with unknown options.	<i>trap-to-host</i>	Forward IPv4 with unknown options to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv4 with unknown options to pass.										
	<i>drop</i>	Drop IPv4 with unknown options.										
<i>trap-to-host</i>	Forward IPv4 with unknown options to FortiOS.											
ipv6-daddr-err	Destination address as unspecified or loopback address anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with destination address as unspecified or loopback address to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with destination address as unspecified or loopback address.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with destination address as unspecified or loopback address to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with destination address as unspecified or loopback address to pass.	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.	<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 with destination address as unspecified or loopback address to pass.										
	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.										
<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.											
ipv6-land	Land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 land attack to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 land attack.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 land attack to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 land attack to pass.	<i>drop</i>	Drop IPv6 land attack.	<i>trap-to-host</i>	Forward IPv6 land attack to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 land attack to pass.										
	<i>drop</i>	Drop IPv6 land attack.										
<i>trap-to-host</i>	Forward IPv6 land attack to FortiOS.											
ipv6-optendpid	End point identification anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with end point identification option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with end point identification option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with end point identification option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with end point identification option to pass.	<i>drop</i>	Drop IPv6 with end point identification option.	<i>trap-to-host</i>	Forward IPv6 with end point identification option to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 with end point identification option to pass.										
	<i>drop</i>	Drop IPv6 with end point identification option.										
<i>trap-to-host</i>	Forward IPv6 with end point identification option to FortiOS.											

Parameter	Description	Type	Size	Default								
ipv6-opthomeaddr	Home address option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with home address option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with home address option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with home address option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with home address option to pass.	drop	Drop IPv6 with home address option.	trap-to-host	Forward IPv6 with home address option to FortiOS.			
Option	Description											
allow	Allow IPv6 with home address option to pass.											
drop	Drop IPv6 with home address option.											
trap-to-host	Forward IPv6 with home address option to FortiOS.											
ipv6-optinvld	Invalid option anomalies.Invalid option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with invalid option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with invalid option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with invalid option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with invalid option to pass.	drop	Drop IPv6 with invalid option.	trap-to-host	Forward IPv6 with invalid option to FortiOS.			
Option	Description											
allow	Allow IPv6 with invalid option to pass.											
drop	Drop IPv6 with invalid option.											
trap-to-host	Forward IPv6 with invalid option to FortiOS.											
ipv6-optjumbo	Jumbo options anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with jumbo option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with jumbo option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with jumbo option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with jumbo option to pass.	drop	Drop IPv6 with jumbo option.	trap-to-host	Forward IPv6 with jumbo option to FortiOS.			
Option	Description											
allow	Allow IPv6 with jumbo option to pass.											
drop	Drop IPv6 with jumbo option.											
trap-to-host	Forward IPv6 with jumbo option to FortiOS.											
ipv6-optnsap	Network service access point address option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with network service access point address option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with network service access point address option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with network service access point address option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with network service access point address option to pass.	drop	Drop IPv6 with network service access point address option.	trap-to-host	Forward IPv6 with network service access point address option to FortiOS.			
Option	Description											
allow	Allow IPv6 with network service access point address option to pass.											
drop	Drop IPv6 with network service access point address option.											
trap-to-host	Forward IPv6 with network service access point address option to FortiOS.											
ipv6-optralert	Router alert option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with router alert option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with router alert option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with router alert option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with router alert option to pass.	drop	Drop IPv6 with router alert option.	trap-to-host	Forward IPv6 with router alert option to FortiOS.			
Option	Description											
allow	Allow IPv6 with router alert option to pass.											
drop	Drop IPv6 with router alert option.											
trap-to-host	Forward IPv6 with router alert option to FortiOS.											

Parameter	Description	Type	Size	Default								
ipv6-opttunnel	Tunnel encapsulation limit option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with tunnel encapsulation limit to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with tunnel encapsulation limit.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with tunnel encapsulation limit to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with tunnel encapsulation limit to pass.	drop	Drop IPv6 with tunnel encapsulation limit.	trap-to-host	Forward IPv6 with tunnel encapsulation limit to FortiOS.			
Option	Description											
allow	Allow IPv6 with tunnel encapsulation limit to pass.											
drop	Drop IPv6 with tunnel encapsulation limit.											
trap-to-host	Forward IPv6 with tunnel encapsulation limit to FortiOS.											
ipv6-proto-err	Layer 4 invalid protocol anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 L4 invalid protocol to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 L4 invalid protocol.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 L4 invalid protocol to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 L4 invalid protocol to pass.	drop	Drop IPv6 L4 invalid protocol.	trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.			
Option	Description											
allow	Allow IPv6 L4 invalid protocol to pass.											
drop	Drop IPv6 L4 invalid protocol.											
trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.											
ipv6-saddr-err	Source address as multicast anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with source address as multicast to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with source address as multicast.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with source address as multicast to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with source address as multicast to pass.	drop	Drop IPv6 with source address as multicast.	trap-to-host	Forward IPv6 with source address as multicast to FortiOS.			
Option	Description											
allow	Allow IPv6 with source address as multicast to pass.											
drop	Drop IPv6 with source address as multicast.											
trap-to-host	Forward IPv6 with source address as multicast to FortiOS.											
ipv6-unknpt	Unknown option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with unknown options to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with unknown options.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with unknown options to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with unknown options to pass.	drop	Drop IPv6 with unknown options.	trap-to-host	Forward IPv6 with unknown options to FortiOS.			
Option	Description											
allow	Allow IPv6 with unknown options to pass.											
drop	Drop IPv6 with unknown options.											
trap-to-host	Forward IPv6 with unknown options to FortiOS.											
tcp-csum-err	Invalid IPv4 TCP checksum anomalies.	option	-	drop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid TCP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid TCP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid TCP checksum.	trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.					
Option	Description											
drop	Drop IPv4 invalid TCP checksum.											
trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.											
tcp-fin-noack	TCP SYN flood with FIN flag set without ACK setting anomalies.	option	-	trap-to-host								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow TCP packets with FIN flag set without ack setting to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set without ack setting.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set without ack setting to FortiOS.		
tcp-fin-only	TCP SYN flood with only FIN flag set anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow TCP packets with FIN flag set only to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set only.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set only to FortiOS.		
tcp-land	TCP land anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow TCP land attack to pass.		
	<i>drop</i>	Drop TCP land attack.		
	<i>trap-to-host</i>	Forward TCP land attack to FortiOS.		
tcp-no-flag	TCP SYN flood with no flag set anomalies.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow TCP packets without flag set to pass.		
	<i>drop</i>	Drop TCP packets without flag set.		
	<i>trap-to-host</i>	Forward TCP packets without flag set to FortiOS.		
tcp-syn-data	TCP SYN flood packets with data anomalies.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow TCP syn packets with data to pass.		
	<i>drop</i>	Drop TCP syn packets with data.		
	<i>trap-to-host</i>	Forward TCP syn packets with data to FortiOS.		
tcp-syn-fin	TCP SYN flood SYN/FIN flag set anomalies.	option	-	allow

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow TCP packets with syn_fin flag set to pass.		
	<i>drop</i>	Drop TCP packets with syn_fin flag set.		
	<i>trap-to-host</i>	Forward TCP packets with syn_fin flag set to FortiOS.		
tcp-winnuke	TCP WinNuke anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow TCP packets winnuke attack to pass.		
	<i>drop</i>	Drop TCP packets winnuke attack.		
	<i>trap-to-host</i>	Forward TCP packets winnuke attack to FortiOS.		
udp-csum-err	Invalid IPv4 UDP checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP checksum to main CPU for processing.		
udp-land	UDP land anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow UDP land attack to pass.		
	<i>drop</i>	Drop UDP land attack.		
	<i>trap-to-host</i>	Forward UDP land attack to FortiOS.		

config hpe

Parameter	Description	Type	Size	Default
arp-max	Maximum ARP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 10000000000	200000
enable-shaper	Enable/Disable NPU host protection engine (HPE) shaper.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable NPU HPE shaping based on packet type.		
	<i>enable</i>	Enable NPU HPE shaping based on packet type.		
esp-max	Maximum ESP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
icmp-max	Maximum ICMP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
ip-frag-max	Maximum fragmented IP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
ip-others-max	Maximum IP packet rate for other packets (packet types that cannot be set with other options) (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
l2-others-max	Maximum L2 packet rate for L2 packets that are not ARP packets (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000
pri-type-max	Maximum overflow rate of priority type traffic (1K - 1G pps, default = 200K pps). Includes L2: HA, 802.3ad LACP, heartbeats. L3: OSPF. L4_TCP: BGP. L4_UDP: IKE, SLBC, BFD.	integer	Minimum value: 1000 Maximum value: 1000000000	200000
sctp-max	Maximum SCTP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000	200000

Parameter	Description	Type	Size	Default
tcp-others-max	Maximum TCP packet rate for TCP packets that match none of the 3 types above (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 10000000000	600000
tcpfin-rst-max	Maximum TCP carries FIN or RST flags packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 10000000000	600000
tcpsyn-ack-max	Maximum TCP carries SYN and ACK flags packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 10000000000	600000
tcpsyn-max	Maximum TCP SYN only packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 10000000000	600000
udp-max	Maximum UDP packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 10000000000	600000

config system npu



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

Configure NPU attributes.

```
config system npu
  Description: Configure NPU attributes.
  set capwap-offload [enable|disable]
  set dedicated-lacp-queue [enable|disable]
  set dedicated-management-affinity {string}
  set dedicated-management-cpu [enable|disable]
  set default-qos-type [policing|shaping|...]
  config dos-options
    Description: NPU DoS configurations.
    set npu-dos-meter-mode [global|local]
    set npu-dos-tpe-mode [enable|disable]
  end
  set double-level-mcast-offload [enable|disable]
  config dsw-dts-profile
    Description: Configure NPU DSW DTS profile.
    edit <profile-id>
      set action [wait|drop|...]
      set min-limit {integer}
      set step {integer}
    next
  end
  config dsw-queue-dts-profile
```

```

Description: Configure NPU DSW Queue DTS profile.
edit <name>
    set iport [eif0|eif1|...]
    set oport [eif0|eif1|...]
    set profile-id {integer}
    set queue-select {integer}
next
end
set fastpath [disable|enable]
config fp-anomaly
    Description: IPv4/IPv6 anomaly protection.
    set gre-csum-err [allow|drop|...]
    set icmp-csum-err [drop|trap-to-host]
    set icmp-frag [allow|drop|...]
    set icmp-land [allow|drop|...]
    set ipv4-csum-err [drop|trap-to-host]
    set ipv4-land [allow|drop|...]
    set ipv4-optlsrr [allow|drop|...]
    set ipv4-optrr [allow|drop|...]
    set ipv4-optsecurity [allow|drop|...]
    set ipv4-optssrr [allow|drop|...]
    set ipv4-optstream [allow|drop|...]
    set ipv4-opttimestamp [allow|drop|...]
    set ipv4-proto-err [allow|drop|...]
    set ipv4-unknopt [allow|drop|...]
    set ipv6-daddr-err [allow|drop|...]
    set ipv6-land [allow|drop|...]
    set ipv6-optendpid [allow|drop|...]
    set ipv6-opthomeaddr [allow|drop|...]
    set ipv6-optinvld [allow|drop|...]
    set ipv6-optjumbo [allow|drop|...]
    set ipv6-optnsap [allow|drop|...]
    set ipv6-optralert [allow|drop|...]
    set ipv6-opttunnel [allow|drop|...]
    set ipv6-proto-err [allow|drop|...]
    set ipv6-saddr-err [allow|drop|...]
    set ipv6-unknopt [allow|drop|...]
    set sctp-csum-err [allow|drop|...]
    set tcp-csum-err [drop|trap-to-host]
    set tcp-fin-noack [allow|drop|...]
    set tcp-fin-only [allow|drop|...]
    set tcp-land [allow|drop|...]
    set tcp-no-flag [allow|drop|...]
    set tcp-syn-data [allow|drop|...]
    set tcp-syn-fin [allow|drop|...]
    set tcp-winnuke [allow|drop|...]
    set udp-csum-err [drop|trap-to-host]
    set udp-land [allow|drop|...]
    set udplite-csum-err [allow|drop|...]
end
set gtp-enhanced-cpu-range [0|1|...]
set gtp-enhanced-mode [enable|disable]

```



```

set gtp-support [enable|disable]
set hash-tbl-spread [enable|disable]
set host-shortcut-mode [bi-directional|host-shortcut]
config hpe
    Description: Host protection engine configuration.
    set all-protocol {integer}
    set arp-max {integer}
    set enable-shaper [disable|enable]
    set esp-max {integer}
    set high-priority {integer}
    set icmp-max {integer}
    set ip-frag-max {integer}
    set ip-others-max {integer}
    set l2-others-max {integer}
    set sctp-max {integer}
    set tcp-max {integer}
    set tcpfin-rst-max {integer}
    set tcpsyn-ack-max {integer}
    set tcpsyn-max {integer}
    set udp-max {integer}
end
set htab-dedi-queue-nr {integer}
set htab-msg-queue [data|idle|...]
set htx-gtse-quota [100Mbps|200Mbps|...]
set htx-icmp-csum-chk [drop|pass]
set inbound-dscp-copy-port <interface1>, <interface2>, ...
set intf-shaping-offload [enable|disable]
set ip-fragment-offload [disable|enable]
config ip-reassembly
    Description: IP reassembly engine configuration.
    set max-timeout {integer}
    set min-timeout {integer}
    set status [disable|enable]
end
set iph-rsvd-re-cksum [enable|disable]
set ipsec-STS-timeout [1|2|...]
set ipsec-dec-subengine-mask {user}
set ipsec-enc-subengine-mask {user}
set ipsec-inbound-cache [enable|disable]
set ipsec-mtu-override [disable|enable]
set ipsec-ob-np-sel [rr|Packet|...]
set ipsec-over-vlink [enable|disable]
set ipsec-throughput-msg-frequency [disable|32KB|...]
set ipt-STS-timeout [1|2|...]
set ipt-throughput-msg-frequency [disable|32KB|...]
config isf-np-queues
    Description: Configure queues of switch port connected to NP6 XAUI on ingress path.
    set cos0 {string}
    set cos1 {string}
    set cos2 {string}
    set cos3 {string}
    set cos4 {string}

```

```

    set cos5 {string}
    set cos6 {string}
    set cos7 {string}
end
set lag-out-port-select [disable|enable]
set max-receive-unit {integer}
set max-session-timeout {integer}
set mcast-session-accounting [tpe-based|session-based|...]
set napi-break-interval {integer}
config np-queues
    Description: Configure queue assignment on NP7.
    config ethernet-type
        Description: Configure a NP7 QoS Ethernet Type.
        edit <name>
            set queue {integer}
            set type {ether-type}
            set weight {integer}
        next
    end
config ip-protocol
    Description: Configure a NP7 QoS IP Protocol.
    edit <name>
        set protocol {integer}
        set queue {integer}
        set weight {integer}
    next
end
config ip-service
    Description: Configure a NP7 QoS IP Service.
    edit <name>
        set dport {integer}
        set protocol {integer}
        set queue {integer}
        set sport {integer}
        set weight {integer}
    next
end
config profile
    Description: Configure a NP7 class profile.
    edit <id>
        set cos0 [queue0|queue1|...]
        set cos1 [queue0|queue1|...]
        set cos2 [queue0|queue1|...]
        set cos3 [queue0|queue1|...]
        set cos4 [queue0|queue1|...]
        set cos5 [queue0|queue1|...]
        set cos6 [queue0|queue1|...]
        set cos7 [queue0|queue1|...]
        set dscp0 [queue0|queue1|...]
        set dscp1 [queue0|queue1|...]
        set dscp10 [queue0|queue1|...]
        set dscp11 [queue0|queue1|...]
    
```

```
set dscp12 [queue0|queue1|...]
set dscp13 [queue0|queue1|...]
set dscp14 [queue0|queue1|...]
set dscp15 [queue0|queue1|...]
set dscp16 [queue0|queue1|...]
set dscp17 [queue0|queue1|...]
set dscp18 [queue0|queue1|...]
set dscp19 [queue0|queue1|...]
set dscp2 [queue0|queue1|...]
set dscp20 [queue0|queue1|...]
set dscp21 [queue0|queue1|...]
set dscp22 [queue0|queue1|...]
set dscp23 [queue0|queue1|...]
set dscp24 [queue0|queue1|...]
set dscp25 [queue0|queue1|...]
set dscp26 [queue0|queue1|...]
set dscp27 [queue0|queue1|...]
set dscp28 [queue0|queue1|...]
set dscp29 [queue0|queue1|...]
set dscp3 [queue0|queue1|...]
set dscp30 [queue0|queue1|...]
set dscp31 [queue0|queue1|...]
set dscp32 [queue0|queue1|...]
set dscp33 [queue0|queue1|...]
set dscp34 [queue0|queue1|...]
set dscp35 [queue0|queue1|...]
set dscp36 [queue0|queue1|...]
set dscp37 [queue0|queue1|...]
set dscp38 [queue0|queue1|...]
set dscp39 [queue0|queue1|...]
set dscp4 [queue0|queue1|...]
set dscp40 [queue0|queue1|...]
set dscp41 [queue0|queue1|...]
set dscp42 [queue0|queue1|...]
set dscp43 [queue0|queue1|...]
set dscp44 [queue0|queue1|...]
set dscp45 [queue0|queue1|...]
set dscp46 [queue0|queue1|...]
set dscp47 [queue0|queue1|...]
set dscp48 [queue0|queue1|...]
set dscp49 [queue0|queue1|...]
set dscp5 [queue0|queue1|...]
set dscp50 [queue0|queue1|...]
set dscp51 [queue0|queue1|...]
set dscp52 [queue0|queue1|...]
set dscp53 [queue0|queue1|...]
set dscp54 [queue0|queue1|...]
set dscp55 [queue0|queue1|...]
set dscp56 [queue0|queue1|...]
set dscp57 [queue0|queue1|...]
set dscp58 [queue0|queue1|...]
set dscp59 [queue0|queue1|...]
```

```

        set dscp6 [queue0|queue1|...]
        set dscp60 [queue0|queue1|...]
        set dscp61 [queue0|queue1|...]
        set dscp62 [queue0|queue1|...]
        set dscp63 [queue0|queue1|...]
        set dscp7 [queue0|queue1|...]
        set dscp8 [queue0|queue1|...]
        set dscp9 [queue0|queue1|...]
        set type [cos|dscp]
        set weight {integer}
    next
end
config scheduler
    Description: Configure a NP7 QoS Scheduler.
    edit <name>
        set mode [none|priority|...]
    next
end
end
set np6-cps-optimization-mode [enable|disable]
config npu-tcam
    Description: Configure NPU TCAM policies.
    edit <name>
        config data
            Description: Data fields of TCAM.
            set df [enable|disable]
            set dstip {ipv4-address-any}
            set dstipv6 {ipv6-address}
            set dstmac {mac-address}
            set dstport {integer}
            set ethertype {ether-type}
            set ext-tag [enable|disable]
            set frag-off {integer}
            set gen-buf-cnt {integer}
            set gen-iv [valid|invalid]
            set gen-l3-flags {integer}
            set gen-l4-flags {integer}
            set gen-pkt-ctrl {integer}
            set gen-pri {integer}
            set gen-pri-v [valid|invalid]
            set gen-tv [valid|invalid]
            set ihl {integer}
            set ip4-id {integer}
            set ip6-fl {integer}
            set ipver {integer}
            set l4-wd10 {integer}
            set l4-wd11 {integer}
            set l4-wd8 {integer}
            set l4-wd9 {integer}
            set mf [enable|disable]
            set protocol {integer}
            set slink {integer}

```

```

set smac-change [enable|disable]
set sp {integer}
set src-cfi [enable|disable]
set src-prio {integer}
set src-updt [enable|disable]
set srcip {ipv4-address-any}
set srcipv6 {ipv6-address}
set srcmac {mac-address}
set srcport {integer}
set svid {integer}
set tcp-ack [enable|disable]
set tcp-cwr [enable|disable]
set tcp-ece [enable|disable]
set tcp-fin [enable|disable]
set tcp-push [enable|disable]
set tcp-rst [enable|disable]
set tcp-syn [enable|disable]
set tcp-urg [enable|disable]
set tgt-cfi [enable|disable]
set tgt-prio {integer}
set tgt-updt [enable|disable]
set tgt-v [valid|invalid]
set tos {integer}
set tp {integer}
set ttl {integer}
set tvid {integer}
set vdid {integer}
end
config mask
Description: Mask fields of TCAM.
set df [enable|disable]
set dstip {ipv4-address-any}
set dstipv6 {ipv6-address}
set dstmac {mac-address}
set dstport {integer}
set ethertype {ether-type}
set ext-tag [enable|disable]
set frag-off {integer}
set gen-buf-cnt {integer}
set gen-iv [valid|invalid]
set gen-l3-flags {integer}
set gen-l4-flags {integer}
set gen-pkt-ctrl {integer}
set gen-pri {integer}
set gen-pri-v [valid|invalid]
set gen-tv [valid|invalid]
set ihl {integer}
set ip4-id {integer}
set ip6-fl {integer}
set ipver {integer}
set l4-wd10 {integer}
set l4-wd11 {integer}

```

```

set l4-wd8 {integer}
set l4-wd9 {integer}
set mf [enable|disable]
set protocol {integer}
set slink {integer}
set smac-change [enable|disable]
set sp {integer}
set src-cfi [enable|disable]
set src-prio {integer}
set src-updt [enable|disable]
set srcip {ipv4-address-any}
set srcipv6 {ipv6-address}
set srcmac {mac-address}
set srcport {integer}
set svid {integer}
set tcp-ack [enable|disable]
set tcp-cwr [enable|disable]
set tcp-ece [enable|disable]
set tcp-fin [enable|disable]
set tcp-push [enable|disable]
set tcp-rst [enable|disable]
set tcp-syn [enable|disable]
set tcp-urg [enable|disable]
set tgt-cfi [enable|disable]
set tgt-prio {integer}
set tgt-updt [enable|disable]
set tgt-v [valid|invalid]
set tos {integer}
set tp {integer}
set ttl {integer}
set tvid {integer}
set vdid {integer}
end
config mir-act
    Description: Mirror action of TCAM.
    set vlif {integer}
end
set oid {integer}
config pri-act
    Description: Priority action of TCAM.
    set priority {integer}
    set weight {integer}
end
config sact
    Description: Source action of TCAM.
    set act {integer}
    set act-v [enable|disable]
    set bmproc {integer}
    set bmproc-v [enable|disable]
    set df-lif {integer}
    set df-lif-v [enable|disable]
    set dfr {integer}

```

```
set dfr-v [enable|disable]
set dmac-skip {integer}
set dmac-skip-v [enable|disable]
set dosen {integer}
set dosen-v [enable|disable]
set espff-proc {integer}
set espff-proc-v [enable|disable]
set etype-pid {integer}
set etype-pid-v [enable|disable]
set frag-proc {integer}
set frag-proc-v [enable|disable]
set fwd {integer}
set fwd-lif {integer}
set fwd-lif-v [enable|disable]
set fwd-tvid {integer}
set fwd-tvid-v [enable|disable]
set fwd-v [enable|disable]
set icpen {integer}
set icpen-v [enable|disable]
set igmp-mld-snp {integer}
set igmp-mld-snp-v [enable|disable]
set learn {integer}
set learn-v [enable|disable]
set m-srh-ctrl {integer}
set m-srh-ctrl-v [enable|disable]
set mac-id {integer}
set mac-id-v [enable|disable]
set mss {integer}
set mss-v [enable|disable]
set pleen {integer}
set pleen-v [enable|disable]
set prio-pid {integer}
set prio-pid-v [enable|disable]
set promis {integer}
set promis-v [enable|disable]
set rfsh {integer}
set rfsh-v [enable|disable]
set smac-skip {integer}
set smac-skip-v [enable|disable]
set tp-smchk-v [enable|disable]
set tp_smchk {integer}
set tpe-id {integer}
set tpe-id-v [enable|disable]
set vdm {integer}
set vdm-v [enable|disable]
set vdom-id {integer}
set vdom-id-v [enable|disable]
set x-mode {integer}
set x-mode-v [enable|disable]
end
config tact
    Description: Target action of TCAM.
```

```

        set act {integer}
        set act-v [enable|disable]
        set fmtuv4-s {integer}
        set fmtuv4-s-v [enable|disable]
        set fmtuv6-s {integer}
        set fmtuv6-s-v [enable|disable]
        set lnkid {integer}
        set lnkid-v [enable|disable]
        set mac-id {integer}
        set mac-id-v [enable|disable]
        set mss-t {integer}
        set mss-t-v [enable|disable]
        set mtuv4 {integer}
        set mtuv4-v [enable|disable]
        set mtuv6 {integer}
        set mtuv6-v [enable|disable]
        set slif-act {integer}
        set slif-act-v [enable|disable]
        set sublnkid {integer}
        set sublnkid-v [enable|disable]
        set tgtv-act {integer}
        set tgtv-act-v [enable|disable]
        set tlif-act {integer}
        set tlif-act-v [enable|disable]
        set tpeid {integer}
        set tpeid-v [enable|disable]
        set v6fe {integer}
        set v6fe-v [enable|disable]
        set vep-en-v [enable|disable]
        set vep-slid {integer}
        set vep-slid-v [enable|disable]
        set vep_en {integer}
        set xlt-lif {integer}
        set xlt-lif-v [enable|disable]
        set xlt-vid {integer}
        set xlt-vid-v [enable|disable]
    end
    set type [L2_src_tc|L2_tgt_tc|...]
    set vid {integer}
next
end
set per-policy-accounting [disable|enable]
set per-session-accounting [traffic-log-only|disable|...]
config port-cpu-map
    Description: Configure NPU interface to CPU core mapping.
    edit <interface>
        set cpu-core {string}
    next
end
config port-npu-map
    Description: Configure port to NPU group mapping.
    edit <interface>

```



```

        set npu-group-index {integer}
    next
end
config port-path-option
    Description: Configure port using NPU or Intel-NIC.
    set ports-using-npu <interface-name1>, <interface-name2>, ...
end
config priority-protocol
    Description: Configure NPU priority protocol.
    set bfd [enable|disable]
    set bgp [enable|disable]
    set slbc [enable|disable]
end
set qos-mode [disable|priority|...]
set qtm-buf-mode [6ch|4ch]
set rdp-offload [enable|disable]
set session-acct-interval {integer}
set session-denied-offload [disable|enable]
set shaping-stats [disable|enable]
set split-ipsec-engines [disable|enable]
set sse-backpressure [enable|disable]
set strip-clear-text-padding [enable|disable]
set strip-esp-padding [enable|disable]
config sw-eh-hash
    Description: Configure switch enhanced hashing.
    set computation [xor16|xor8|...]
    set destination-ip-lower-16 [include|exclude]
    set destination-ip-upper-16 [include|exclude]
    set destination-port [include|exclude]
    set ip-protocol [include|exclude]
    set netmask-length {integer}
    set source-ip-lower-16 [include|exclude]
    set source-ip-upper-16 [include|exclude]
    set source-port [include|exclude]
end
set sw-np-bandwidth [0G|2G|...]
config sw-tr-hash
    Description: Configure switch traditional hashing.
    set draco15 [enable|disable]
    set tcp-udp-port [include|exclude]
end
set switch-np-hash [src-ip|dst-ip|...]
set tunnel-over-vlink [enable|disable]
set uesp-offload [enable|disable]
set ull-port-mode [10G|25G]
set vlan-lookup-cache [enable|disable]
set vxlan-offload [enable|disable]
end

```

config system npu

Parameter	Description	Type	Size	Default								
capwap-offload *	Enable/disable offloading managed FortiAP and FortiLink CAPWAP sessions.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable CAPWAP offload.</td></tr><tr><td>disable</td><td>Disable CAPWAP offload.</td></tr></table>	Option	Description	enable	Enable CAPWAP offload.	disable	Disable CAPWAP offload.					
Option	Description											
enable	Enable CAPWAP offload.											
disable	Disable CAPWAP offload.											
dedicated-lacp-queue *	Enable/disable dedication of HIF queue #0 for LACP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dedication of HIF queue #0 for LACP.</td></tr><tr><td>disable</td><td>Disable dedication of HIF queue #0 for LACP.</td></tr></table>	Option	Description	enable	Enable dedication of HIF queue #0 for LACP.	disable	Disable dedication of HIF queue #0 for LACP.					
Option	Description											
enable	Enable dedication of HIF queue #0 for LACP.											
disable	Disable dedication of HIF queue #0 for LACP.											
dedicated-management-affinity *	Affinity setting for management daemons (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1								
dedicated-management-cpu *	Enable to dedicate one CPU for GUI and CLI connections when NPs are busy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dedication of CPU #0 for management tasks.</td></tr><tr><td>disable</td><td>Disable dedication of CPU #0 for management tasks.</td></tr></table>	Option	Description	enable	Enable dedication of CPU #0 for management tasks.	disable	Disable dedication of CPU #0 for management tasks.					
Option	Description											
enable	Enable dedication of CPU #0 for management tasks.											
disable	Disable dedication of CPU #0 for management tasks.											
default-qos-type *	Set default QoS type.	option	-	policing								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>policing</td><td>QoS type policing.</td></tr><tr><td>shaping</td><td>QoS type shaping.</td></tr><tr><td>policing-enhanced</td><td>Enhanced QoS type policing.</td></tr></table>	Option	Description	policing	QoS type policing.	shaping	QoS type shaping.	policing-enhanced	Enhanced QoS type policing.			
Option	Description											
policing	QoS type policing.											
shaping	QoS type shaping.											
policing-enhanced	Enhanced QoS type policing.											
double-level-mcast-offload *	Enable double level mcast offload.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable double level mcast offload.</td></tr></table>	Option	Description	enable	Enable double level mcast offload.							
Option	Description											
enable	Enable double level mcast offload.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable double level mcast offload.		
fastpath *	Enable/disable NP6 offloading (also called fast path).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable NP6 offloading (fast path).		
	<i>enable</i>	Enable NP6 offloading (fast path).		
gtp-enhanced-cpu-range *	GTP enhanced CPU range option.	option	-	0
	Option	Description		
	0	Inspect GTPU packets by all CPUs.		
	1	Inspect GTPU packets by Master CPUs.		
	2	Inspect GTPU packets by Slave CPUs.		
gtp-enhanced-mode *	Enable/disable GTP enhanced mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable GTP enhanced mode.		
	<i>disable</i>	Disable GTP enhanced mode.		
gtp-support *	Enable/Disable NP7 GTP support	option	-	disable
	Option	Description		
	<i>enable</i>	Enable NP7 GTP support		
	<i>disable</i>	Disable NP7 GTP support		
hash-tbl-spread *	Enable/disable hash table entry spread (default enabled).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable hash table entry spread.		
	<i>disable</i>	Disable hash table entry spread.		
host-shortcut-mode *	Set NP6 host shortcut mode.	option	-	bi-directional

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bi-directional</i></td><td>Offload TCP and IP Tunnel sessions in both directions between 10G and 1G interfaces (normal operation).</td></tr><tr><td><i>host-shortcut</i></td><td>Only offload TCP and IP Tunnel sessions received by 1G interfaces. Select if packets are dropped for offloaded traffic between 10G to 1G interfaces.</td></tr></table>	Option	Description	<i>bi-directional</i>	Offload TCP and IP Tunnel sessions in both directions between 10G and 1G interfaces (normal operation).	<i>host-shortcut</i>	Only offload TCP and IP Tunnel sessions received by 1G interfaces. Select if packets are dropped for offloaded traffic between 10G to 1G interfaces.																							
	Option	Description																												
	<i>bi-directional</i>	Offload TCP and IP Tunnel sessions in both directions between 10G and 1G interfaces (normal operation).																												
<i>host-shortcut</i>	Only offload TCP and IP Tunnel sessions received by 1G interfaces. Select if packets are dropped for offloaded traffic between 10G to 1G interfaces.																													
htab-dedi-queue-nr *	Set the number of dedicate queue for hash table messages.	integer	Minimum value: 1 Maximum value: 2	1																										
htab-msg-queue *	Set hash table message queue mode.	option	-	data																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>data</i></td><td>Use data queue.</td></tr><tr><td><i>idle</i></td><td>Use idle queue.</td></tr><tr><td><i>dedicated</i></td><td>Use dedicated queue.</td></tr></table>	Option	Description	<i>data</i>	Use data queue.	<i>idle</i>	Use idle queue.	<i>dedicated</i>	Use dedicated queue.																					
	Option	Description																												
	<i>data</i>	Use data queue.																												
	<i>idle</i>	Use idle queue.																												
<i>dedicated</i>	Use dedicated queue.																													
htx-gtse-quota *	Configure HTX GTSE quota.	option	-	1Gbps																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>100Mbps</i></td><td>100Mbps.</td></tr><tr><td><i>200Mbps</i></td><td>200Mbps.</td></tr><tr><td><i>300Mbps</i></td><td>300Mbps.</td></tr><tr><td><i>400Mbps</i></td><td>400Mbps.</td></tr><tr><td><i>500Mbps</i></td><td>500Mbps.</td></tr><tr><td><i>600Mbps</i></td><td>600Mbps.</td></tr><tr><td><i>700Mbps</i></td><td>700Mbps.</td></tr><tr><td><i>800Mbps</i></td><td>800Mbps.</td></tr><tr><td><i>900Mbps</i></td><td>900Mbps.</td></tr><tr><td><i>1Gbps</i></td><td>1Gbps.</td></tr><tr><td><i>2Gbps</i></td><td>2Gbps.</td></tr><tr><td><i>4Gbps</i></td><td>4Gbps.</td></tr></table>	Option	Description	<i>100Mbps</i>	100Mbps.	<i>200Mbps</i>	200Mbps.	<i>300Mbps</i>	300Mbps.	<i>400Mbps</i>	400Mbps.	<i>500Mbps</i>	500Mbps.	<i>600Mbps</i>	600Mbps.	<i>700Mbps</i>	700Mbps.	<i>800Mbps</i>	800Mbps.	<i>900Mbps</i>	900Mbps.	<i>1Gbps</i>	1Gbps.	<i>2Gbps</i>	2Gbps.	<i>4Gbps</i>	4Gbps.			
	Option	Description																												
	<i>100Mbps</i>	100Mbps.																												
	<i>200Mbps</i>	200Mbps.																												
	<i>300Mbps</i>	300Mbps.																												
	<i>400Mbps</i>	400Mbps.																												
	<i>500Mbps</i>	500Mbps.																												
	<i>600Mbps</i>	600Mbps.																												
	<i>700Mbps</i>	700Mbps.																												
	<i>800Mbps</i>	800Mbps.																												
	<i>900Mbps</i>	900Mbps.																												
	<i>1Gbps</i>	1Gbps.																												
	<i>2Gbps</i>	2Gbps.																												
<i>4Gbps</i>	4Gbps.																													

Parameter	Description	Type	Size	Default
	Option	Description		
	8Gbps	8Gbps.		
	10Gbps	10Gbps.		
htx-icmp-csum-chk *	Set HTX icmp csum checking mode.	option	-	drop
	Option	Description		
	drop	Drop bad icmp csum.		
	pass	Pass bad icmp csum.		
inbound-dscp-copy-port <interface> *	Physical interfaces that support inbound-dscp-copy. Physical interface name.	string	Maximum length: 15	
intf-shaping-offload *	Enable/disable NPU offload when doing interface-based traffic shaping according to the egress-shaping-profile.	option	-	disable
	Option	Description		
	enable	Enable NPU offload when doing interface-based traffic shaping according to the egress-shaping-profile.		
	disable	Disable NPU offload when doing interface-based traffic shaping according to the egress-shaping-profile.		
ip-fragment-offload *	Enable/disable NP7 NPU IP fragment offload.	option	-	enable
	Option	Description		
	disable	Disable IP fragment offload.		
	enable	Enable IP fragment offload.		
iph-rsvd-recksum *	Enable/disable IP checksum re-calculation for packets with iph.reserved bit set.	option	-	disable
	Option	Description		
	enable	Enable IP checksum re-calculation for packets with iph.reserved bit set.		
	disable	Disable IP checksum re-calculation for packets with iph.reserved bit set.		

Parameter	Description	Type	Size	Default																						
ipsec-STs-timeout *	Set NP7Lite IPsec STS msg timeout.	option	-	5																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Set NP7Lite STS message timeout to 1 sec(recommended for IPSec throughput GUI).</td></tr><tr><td>2</td><td>Set NP7Lite STS message timeout to 2 sec.</td></tr><tr><td>3</td><td>Set NP7Lite STS message timeout to 3 sec.</td></tr><tr><td>4</td><td>Set NP7Lite STS message timeout to 4 sec.</td></tr><tr><td>5</td><td>Set NP7Lite STS message timeout to 5 sec(default).</td></tr><tr><td>6</td><td>Set NP7Lite STS message timeout to 6 sec.</td></tr><tr><td>7</td><td>Set NP7Lite STS message timeout to 7 sec.</td></tr><tr><td>8</td><td>Set NP7Lite STS message timeout to 8 sec.</td></tr><tr><td>9</td><td>Set NP7Lite STS message timeout to 9 sec.</td></tr><tr><td>10</td><td>Set NP7Lite STS message timeout to 10 sec.</td></tr></table>	Option	Description	1	Set NP7Lite STS message timeout to 1 sec(recommended for IPSec throughput GUI).	2	Set NP7Lite STS message timeout to 2 sec.	3	Set NP7Lite STS message timeout to 3 sec.	4	Set NP7Lite STS message timeout to 4 sec.	5	Set NP7Lite STS message timeout to 5 sec(default).	6	Set NP7Lite STS message timeout to 6 sec.	7	Set NP7Lite STS message timeout to 7 sec.	8	Set NP7Lite STS message timeout to 8 sec.	9	Set NP7Lite STS message timeout to 9 sec.	10	Set NP7Lite STS message timeout to 10 sec.			
	Option	Description																								
	1	Set NP7Lite STS message timeout to 1 sec(recommended for IPSec throughput GUI).																								
	2	Set NP7Lite STS message timeout to 2 sec.																								
	3	Set NP7Lite STS message timeout to 3 sec.																								
	4	Set NP7Lite STS message timeout to 4 sec.																								
	5	Set NP7Lite STS message timeout to 5 sec(default).																								
	6	Set NP7Lite STS message timeout to 6 sec.																								
	7	Set NP7Lite STS message timeout to 7 sec.																								
	8	Set NP7Lite STS message timeout to 8 sec.																								
9	Set NP7Lite STS message timeout to 9 sec.																									
10	Set NP7Lite STS message timeout to 10 sec.																									
ipsec-dec-subengine-mask *	IPsec decryption subengine mask (0x1 - 0xff, default 0xff).	user	Not Specified																							
ipsec-enc-subengine-mask *	IPsec encryption subengine mask (0x1 - 0xff, default 0xff).	user	Not Specified																							
ipsec-inbound-cache *	Enable/disable IPsec inbound cache for anti-replay.	option	-	enable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable inbound cache always.</td></tr><tr><td>disable</td><td>Disable inbound cache when IPsec anti-replay is on.</td></tr></table>	Option	Description	enable	Enable inbound cache always.	disable	Disable inbound cache when IPsec anti-replay is on.																			
	Option	Description																								
enable	Enable inbound cache always.																									
disable	Disable inbound cache when IPsec anti-replay is on.																									
ipsec-mtu-override *	Enable/disable NP6 IPsec MTU override.	option	-	disable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NP6 IPsec MTU override.</td></tr><tr><td>enable</td><td>Enable NP6 IPsec MTU override.</td></tr></table>	Option	Description	disable	Disable NP6 IPsec MTU override.	enable	Enable NP6 IPsec MTU override.																			
	Option	Description																								
disable	Disable NP6 IPsec MTU override.																									
enable	Enable NP6 IPsec MTU override.																									
ipsec-ob-np-sel *	IPsec NP selection for OB SA offloading.	option	-	rr																						

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rr</i></td><td>Round Robin.</td></tr><tr><td><i>Packet</i></td><td>NPU of the first packet.</td></tr><tr><td><i>Hash</i></td><td>Hash.</td></tr></table>	Option	Description	<i>rr</i>	Round Robin.	<i>Packet</i>	NPU of the first packet.	<i>Hash</i>	Hash.																															
	Option	Description																																						
	<i>rr</i>	Round Robin.																																						
	<i>Packet</i>	NPU of the first packet.																																						
<i>Hash</i>	Hash.																																							
ipsec-over-vlink *	Enable/disable IPsec over vlink.	option	-	disable																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPSEC over vlink.</td></tr><tr><td><i>disable</i></td><td>Disable IPSEC over vlink.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPSEC over vlink.	<i>disable</i>	Disable IPSEC over vlink.																																	
	Option	Description																																						
	<i>enable</i>	Enable IPSEC over vlink.																																						
<i>disable</i>	Disable IPSEC over vlink.																																							
ipsec-throughput-msg-frequency *	Set NP7Lite IPsec throughput msg frequency: 0--disable 1--32KB 3--64KB ... 0x3fff--256MB 0x7fff--512MB 0xffff--1GB.	option	-	disable																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NP7Lite throughput update message.</td></tr><tr><td><i>32KB</i></td><td>Set NP7Lite throughput update message frequency to 32KB.</td></tr><tr><td><i>64KB</i></td><td>Set NP7Lite throughput update message frequency to 64KB.</td></tr><tr><td><i>128KB</i></td><td>Set NP7Lite throughput update message frequency to 128KB.</td></tr><tr><td><i>256KB</i></td><td>Set NP7Lite throughput update message frequency to 256KB.</td></tr><tr><td><i>512KB</i></td><td>Set NP7Lite throughput update message frequency to 512KB.</td></tr><tr><td><i>1MB</i></td><td>Set NP7Lite throughput update message frequency to 1MB.</td></tr><tr><td><i>2MB</i></td><td>Set NP7Lite throughput update message frequency to 2MB.</td></tr><tr><td><i>4MB</i></td><td>Set NP7Lite throughput update message frequency to 4MB.</td></tr><tr><td><i>8MB</i></td><td>Set NP7Lite throughput update message frequency to 8MB.</td></tr><tr><td><i>16MB</i></td><td>Set NP7Lite throughput update message frequency to 16MB.</td></tr><tr><td><i>32MB</i></td><td>Set NP7Lite throughput update message frequency to 32MB.</td></tr><tr><td><i>64MB</i></td><td>Set NP7Lite throughput update message frequency to 64MB.</td></tr><tr><td><i>128MB</i></td><td>Set NP7Lite throughput update message frequency to 128MB.</td></tr><tr><td><i>256MB</i></td><td>Set NP7Lite throughput update message frequency to 256MB.</td></tr><tr><td><i>512MB</i></td><td>Set NP7Lite throughput update message frequency to 512MB.</td></tr><tr><td><i>1GB</i></td><td>Set NP7Lite throughput update message frequency to 1GB.</td></tr></table>	Option	Description	<i>disable</i>	Disable NP7Lite throughput update message.	<i>32KB</i>	Set NP7Lite throughput update message frequency to 32KB.	<i>64KB</i>	Set NP7Lite throughput update message frequency to 64KB.	<i>128KB</i>	Set NP7Lite throughput update message frequency to 128KB.	<i>256KB</i>	Set NP7Lite throughput update message frequency to 256KB.	<i>512KB</i>	Set NP7Lite throughput update message frequency to 512KB.	<i>1MB</i>	Set NP7Lite throughput update message frequency to 1MB.	<i>2MB</i>	Set NP7Lite throughput update message frequency to 2MB.	<i>4MB</i>	Set NP7Lite throughput update message frequency to 4MB.	<i>8MB</i>	Set NP7Lite throughput update message frequency to 8MB.	<i>16MB</i>	Set NP7Lite throughput update message frequency to 16MB.	<i>32MB</i>	Set NP7Lite throughput update message frequency to 32MB.	<i>64MB</i>	Set NP7Lite throughput update message frequency to 64MB.	<i>128MB</i>	Set NP7Lite throughput update message frequency to 128MB.	<i>256MB</i>	Set NP7Lite throughput update message frequency to 256MB.	<i>512MB</i>	Set NP7Lite throughput update message frequency to 512MB.	<i>1GB</i>	Set NP7Lite throughput update message frequency to 1GB.			
	Option	Description																																						
	<i>disable</i>	Disable NP7Lite throughput update message.																																						
	<i>32KB</i>	Set NP7Lite throughput update message frequency to 32KB.																																						
	<i>64KB</i>	Set NP7Lite throughput update message frequency to 64KB.																																						
	<i>128KB</i>	Set NP7Lite throughput update message frequency to 128KB.																																						
	<i>256KB</i>	Set NP7Lite throughput update message frequency to 256KB.																																						
	<i>512KB</i>	Set NP7Lite throughput update message frequency to 512KB.																																						
	<i>1MB</i>	Set NP7Lite throughput update message frequency to 1MB.																																						
	<i>2MB</i>	Set NP7Lite throughput update message frequency to 2MB.																																						
	<i>4MB</i>	Set NP7Lite throughput update message frequency to 4MB.																																						
	<i>8MB</i>	Set NP7Lite throughput update message frequency to 8MB.																																						
	<i>16MB</i>	Set NP7Lite throughput update message frequency to 16MB.																																						
	<i>32MB</i>	Set NP7Lite throughput update message frequency to 32MB.																																						
	<i>64MB</i>	Set NP7Lite throughput update message frequency to 64MB.																																						
	<i>128MB</i>	Set NP7Lite throughput update message frequency to 128MB.																																						
	<i>256MB</i>	Set NP7Lite throughput update message frequency to 256MB.																																						
<i>512MB</i>	Set NP7Lite throughput update message frequency to 512MB.																																							
<i>1GB</i>	Set NP7Lite throughput update message frequency to 1GB.																																							

Parameter	Description	Type	Size	Default																										
ipt-STS-timeout *	Set NP7Lite IPT STS msg timeout.	option	-	5																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Set NP7Lite STS message timeout to 1 sec(recommended for IPSec throughput GUI).</td></tr><tr><td>2</td><td>Set NP7Lite STS message timeout to 2 sec.</td></tr><tr><td>3</td><td>Set NP7Lite STS message timeout to 3 sec.</td></tr><tr><td>4</td><td>Set NP7Lite STS message timeout to 4 sec.</td></tr><tr><td>5</td><td>Set NP7Lite STS message timeout to 5 sec(default).</td></tr><tr><td>6</td><td>Set NP7Lite STS message timeout to 6 sec.</td></tr><tr><td>7</td><td>Set NP7Lite STS message timeout to 7 sec.</td></tr><tr><td>8</td><td>Set NP7Lite STS message timeout to 8 sec.</td></tr><tr><td>9</td><td>Set NP7Lite STS message timeout to 9 sec.</td></tr><tr><td>10</td><td>Set NP7Lite STS message timeout to 10 sec.</td></tr></table>	Option	Description	1	Set NP7Lite STS message timeout to 1 sec(recommended for IPSec throughput GUI).	2	Set NP7Lite STS message timeout to 2 sec.	3	Set NP7Lite STS message timeout to 3 sec.	4	Set NP7Lite STS message timeout to 4 sec.	5	Set NP7Lite STS message timeout to 5 sec(default).	6	Set NP7Lite STS message timeout to 6 sec.	7	Set NP7Lite STS message timeout to 7 sec.	8	Set NP7Lite STS message timeout to 8 sec.	9	Set NP7Lite STS message timeout to 9 sec.	10	Set NP7Lite STS message timeout to 10 sec.							
Option	Description																													
1	Set NP7Lite STS message timeout to 1 sec(recommended for IPSec throughput GUI).																													
2	Set NP7Lite STS message timeout to 2 sec.																													
3	Set NP7Lite STS message timeout to 3 sec.																													
4	Set NP7Lite STS message timeout to 4 sec.																													
5	Set NP7Lite STS message timeout to 5 sec(default).																													
6	Set NP7Lite STS message timeout to 6 sec.																													
7	Set NP7Lite STS message timeout to 7 sec.																													
8	Set NP7Lite STS message timeout to 8 sec.																													
9	Set NP7Lite STS message timeout to 9 sec.																													
10	Set NP7Lite STS message timeout to 10 sec.																													
ipt-throughput- msg-frequency *	Set NP7Lite IPT throughput msg frequency: 0-- disable 1--32KB 3--64KB ... 0x3fff--256MB 0x7fff--512MB 0xffff--1GB.	option	-	disable																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NP7Lite throughput update message.</td></tr><tr><td>32KB</td><td>Set NP7Lite throughput update message frequency to 32KB.</td></tr><tr><td>64KB</td><td>Set NP7Lite throughput update message frequency to 64KB.</td></tr><tr><td>128KB</td><td>Set NP7Lite throughput update message frequency to 128KB.</td></tr><tr><td>256KB</td><td>Set NP7Lite throughput update message frequency to 256KB.</td></tr><tr><td>512KB</td><td>Set NP7Lite throughput update message frequency to 512KB.</td></tr><tr><td>1MB</td><td>Set NP7Lite throughput update message frequency to 1MB.</td></tr><tr><td>2MB</td><td>Set NP7Lite throughput update message frequency to 2MB.</td></tr><tr><td>4MB</td><td>Set NP7Lite throughput update message frequency to 4MB.</td></tr><tr><td>8MB</td><td>Set NP7Lite throughput update message frequency to 8MB.</td></tr><tr><td>16MB</td><td>Set NP7Lite throughput update message frequency to 16MB.</td></tr><tr><td>32MB</td><td>Set NP7Lite throughput update message frequency to 32MB.</td></tr></table>	Option	Description	disable	Disable NP7Lite throughput update message.	32KB	Set NP7Lite throughput update message frequency to 32KB.	64KB	Set NP7Lite throughput update message frequency to 64KB.	128KB	Set NP7Lite throughput update message frequency to 128KB.	256KB	Set NP7Lite throughput update message frequency to 256KB.	512KB	Set NP7Lite throughput update message frequency to 512KB.	1MB	Set NP7Lite throughput update message frequency to 1MB.	2MB	Set NP7Lite throughput update message frequency to 2MB.	4MB	Set NP7Lite throughput update message frequency to 4MB.	8MB	Set NP7Lite throughput update message frequency to 8MB.	16MB	Set NP7Lite throughput update message frequency to 16MB.	32MB	Set NP7Lite throughput update message frequency to 32MB.			
Option	Description																													
disable	Disable NP7Lite throughput update message.																													
32KB	Set NP7Lite throughput update message frequency to 32KB.																													
64KB	Set NP7Lite throughput update message frequency to 64KB.																													
128KB	Set NP7Lite throughput update message frequency to 128KB.																													
256KB	Set NP7Lite throughput update message frequency to 256KB.																													
512KB	Set NP7Lite throughput update message frequency to 512KB.																													
1MB	Set NP7Lite throughput update message frequency to 1MB.																													
2MB	Set NP7Lite throughput update message frequency to 2MB.																													
4MB	Set NP7Lite throughput update message frequency to 4MB.																													
8MB	Set NP7Lite throughput update message frequency to 8MB.																													
16MB	Set NP7Lite throughput update message frequency to 16MB.																													
32MB	Set NP7Lite throughput update message frequency to 32MB.																													

Parameter	Description	Type	Size	Default													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>64MB</td><td>Set NP7Lite throughput update message frequency to 64MB.</td></tr><tr><td>128MB</td><td>Set NP7Lite throughput update message frequency to 128MB.</td></tr><tr><td>256MB</td><td>Set NP7Lite throughput update message frequency to 256MB.</td></tr><tr><td>512MB</td><td>Set NP7Lite throughput update message frequency to 512MB.</td></tr><tr><td>1GB</td><td>Set NP7Lite throughput update message frequency to 1GB.</td></tr></table>		Option	Description	64MB	Set NP7Lite throughput update message frequency to 64MB.	128MB	Set NP7Lite throughput update message frequency to 128MB.	256MB	Set NP7Lite throughput update message frequency to 256MB.	512MB	Set NP7Lite throughput update message frequency to 512MB.	1GB	Set NP7Lite throughput update message frequency to 1GB.			
	Option	Description															
	64MB	Set NP7Lite throughput update message frequency to 64MB.															
	128MB	Set NP7Lite throughput update message frequency to 128MB.															
	256MB	Set NP7Lite throughput update message frequency to 256MB.															
	512MB	Set NP7Lite throughput update message frequency to 512MB.															
1GB	Set NP7Lite throughput update message frequency to 1GB.																
lag-out-port-select *	Enable/disable LAG outgoing port selection based on incoming traffic port.	option	-	disable													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable LAG outgoing trunk in switch.</td></tr><tr><td>enable</td><td>Enable LAG outgoing trunk in switch.</td></tr></table>		Option	Description	disable	Disable LAG outgoing trunk in switch.	enable	Enable LAG outgoing trunk in switch.									
	Option	Description															
	disable	Disable LAG outgoing trunk in switch.															
enable	Enable LAG outgoing trunk in switch.																
max-receive-unit *	Set the maximum packet size for receive, larger packets will be silently dropped.	integer	Minimum value: 64 Maximum value: 10000	10000													
max-session-timeout *	Maximum time interval for refreshing NPU-offloaded sessions (10 - 1000 sec, default 40 sec).	integer	Minimum value: 10 Maximum value: 1000	40													
mcast-session-accounting *	Enable/disable traffic accounting for each multicast session through TAE counter.	option	-	tpe-based													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tpe-based</td><td>Enable TPE-based multicast session accounting.</td></tr><tr><td>session-based</td><td>Enable session-based multicast session accounting.</td></tr><tr><td>disable</td><td>Disable multicast session accounting.</td></tr></table>		Option	Description	tpe-based	Enable TPE-based multicast session accounting.	session-based	Enable session-based multicast session accounting.	disable	Disable multicast session accounting.							
	Option	Description															
	tpe-based	Enable TPE-based multicast session accounting.															
	session-based	Enable session-based multicast session accounting.															
disable	Disable multicast session accounting.																
napi-break-interval *	NAPI break interval (default 0).	integer	Minimum value: 0 Maximum value: 65535	0													
np6-cps-optimization-mode *	Enable/disable NP6 connection per second (CPS) optimization mode.	option	-	disable													

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable NP6 connection per second (CPS) optimization mode.		
	<i>disable</i>	Disable NP6 connection per second (CPS) optimization mode.		
per-policy-accounting *	Set per-policy accounting.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable per-policy hit count.		
	<i>enable</i>	Enable per-policy hit count		
per-session-accounting *	Set per-session accounting.	option	-	traffic-log-only
	Option	Description		
	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging		
	<i>disable</i>	Disable per-session accounting.		
	<i>enable</i>	Per-session accounting for all sessions.		
qos-mode *	QoS mode on switch and NP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable QoS on switch and NP.		
	<i>priority</i>	Priority based.		
	<i>round-robin</i>	Round Robin Scheduler.		
qtm-buf-mode *	QTM channel configuration for packet buffer.	option	-	6ch
	Option	Description		
	<i>6ch</i>	6 DRAM channels for packet buffer.		
	<i>4ch</i>	4 DRAM channels for packet buffer.		
rdp-offload *	Enable/disable RDP offload.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable reliable datagram protocol traffic offload.		
	<i>disable</i>	Disable reliable datagram protocol traffic offload.		

Parameter	Description	Type	Size	Default						
session-acct-interval *	Session accounting update interval (1 - 10 sec, default 5 sec).	integer	Minimum value: 1 Maximum value: 10	5						
session-denied-offload *	Enable/disable offloading of denied sessions. Requires ses-denied-traffic to be set.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable offloading of denied sessions.</td></tr><tr><td>enable</td><td>Enable offloading of denied sessions.</td></tr></table>	Option	Description	disable	Disable offloading of denied sessions.	enable	Enable offloading of denied sessions.			
Option	Description									
disable	Disable offloading of denied sessions.									
enable	Enable offloading of denied sessions.									
shaping-stats *	Enable/disable NP7 traffic shaping statistics (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NP7 traffic shaping statistics.</td></tr><tr><td>enable</td><td>Enable NP7 traffic shaping statistics.</td></tr></table>	Option	Description	disable	Disable NP7 traffic shaping statistics.	enable	Enable NP7 traffic shaping statistics.			
Option	Description									
disable	Disable NP7 traffic shaping statistics.									
enable	Enable NP7 traffic shaping statistics.									
split-ipsec-engines *	Enable/disable Split IPsec Engines.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Split IPsec Engines.</td></tr><tr><td>enable</td><td>Enable Split IPsec Engines.</td></tr></table>	Option	Description	disable	Disable Split IPsec Engines.	enable	Enable Split IPsec Engines.			
Option	Description									
disable	Disable Split IPsec Engines.									
enable	Enable Split IPsec Engines.									
sse-backpressure *	Enable/disable SSE backpressure.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SSE backpressure.</td></tr><tr><td>disable</td><td>Disable SSE backpressure.</td></tr></table>	Option	Description	enable	Enable SSE backpressure.	disable	Disable SSE backpressure.			
Option	Description									
enable	Enable SSE backpressure.									
disable	Disable SSE backpressure.									
strip-clear-text-padding *	Enable/disable stripping clear text padding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable stripping clear text padding.</td></tr><tr><td>disable</td><td>Disable stripping clear text padding.</td></tr></table>	Option	Description	enable	Enable stripping clear text padding.	disable	Disable stripping clear text padding.			
Option	Description									
enable	Enable stripping clear text padding.									
disable	Disable stripping clear text padding.									
strip-esp-padding *	Enable/disable stripping ESP padding.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable stripping ESP padding.		
	<i>disable</i>	Disable stripping ESP padding.		
sw-np-bandwidth *	Bandwidth from switch to NP.	option	-	0G
	Option	Description		
	<i>0G</i>	Default value. No bandwidth control.		
	<i>2G</i>	2Gbps.		
	<i>4G</i>	4Gbps.		
	<i>5G</i>	5Gbps.		
	<i>6G</i>	6Gbps.		
	<i>7G</i>	7Gbps.		
	<i>8G</i>	8Gbps.		
	<i>9G</i>	9Gbps.		
switch-np-hash *	Switch-NP trunk port selection Criteria.	option	-	src-dst-ip
	Option	Description		
	<i>src-ip</i>	Source IP address.		
	<i>dst-ip</i>	Destination IP address.		
	<i>src-dst-ip</i>	Source+dest IP address.		
tunnel-over-vlink *	Enable/disable selection of which NP6 chip the tunnel uses (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Use the bundled NP6 chip for tunnels.		
	<i>disable</i>	Use the ingress NP6 chip for tunnels.		
uesp-offload *	Enable/disable UDP-encapsulated ESP offload (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable UDP-encapsulated ESP traffic offload.		
	<i>disable</i>	Disable UDP-encapsulated ESP traffic offload.		

Parameter	Description	Type	Size	Default						
ull-port-mode *	Set ULL port's speed to 10G/25G (default 10G).	option	-	10G						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>10G</td><td>10G speed setting for ULL ports.</td></tr><tr><td>25G</td><td>25G speed setting for ULL ports.</td></tr></table>	Option	Description	10G	10G speed setting for ULL ports.	25G	25G speed setting for ULL ports.			
Option	Description									
10G	10G speed setting for ULL ports.									
25G	25G speed setting for ULL ports.									
vlan-lookup-cache *	Enable/disable vlan lookup cache (default enabled).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable VLAN lookup cache.</td></tr><tr><td>disable</td><td>Disable VLAN lookup cache.</td></tr></table>	Option	Description	enable	Enable VLAN lookup cache.	disable	Disable VLAN lookup cache.			
Option	Description									
enable	Enable VLAN lookup cache.									
disable	Disable VLAN lookup cache.									
vxlan-offload *	Enable/disable offloading vxlan.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Vxlan offload.</td></tr><tr><td>disable</td><td>Disable Vxlan offload.</td></tr></table>	Option	Description	enable	Enable Vxlan offload.	disable	Disable Vxlan offload.			
Option	Description									
enable	Enable Vxlan offload.									
disable	Disable Vxlan offload.									

* This parameter may not exist in some models.

config dos-options

Parameter	Description	Type	Size	Default						
npu-dos-meter-mode	Set DoS meter NPU offloading mode.	option	-	global						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>global</td><td>Install DoS meter to all NPs.</td></tr><tr><td>local</td><td>Install DoS meter only to the NP assigned to the traffic.</td></tr></table>	Option	Description	global	Install DoS meter to all NPs.	local	Install DoS meter only to the NP assigned to the traffic.			
Option	Description									
global	Install DoS meter to all NPs.									
local	Install DoS meter only to the NP assigned to the traffic.									
npu-dos-tpc-mode	Enable/disable insertion of DoS meter ID to session table.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable insertion of DoS meter ID to session table.</td></tr><tr><td>disable</td><td>Disable insertion of DoS meter ID to session table.</td></tr></table>	Option	Description	enable	Enable insertion of DoS meter ID to session table.	disable	Disable insertion of DoS meter ID to session table.			
Option	Description									
enable	Enable insertion of DoS meter ID to session table.									
disable	Disable insertion of DoS meter ID to session table.									

config dsw-dts-profile

Parameter	Description	Type	Size	Default
action	Set NPU DSW DTS profile action.	option	-	wait
	Option	Description		
	<i>wait</i>	DSW DTS profile WAIT indefinitely.		
	<i>drop</i>	DSW DTS profile DROP immediately.		
	<i>drop_tmr_0</i>	DSW DTS profile DROP after interval #0 time-out.		
	<i>drop_tmr_1</i>	DSW DTS profile DROP after interval #1 time-out.		
	<i>enqueue</i>	DSW DTS profile ENQUE immediately.		
	<i>enqueue_0</i>	DSW DTS profile ENQUE after interval #0 time-out.		
	<i>enqueue_1</i>	DSW DTS profile ENQUE after interval #1 time-out.		
min-limit	Set NPU DSW DTS profile min-limit.	integer	Minimum value: 32 Maximum value: 2048	0
profile-id	Set NPU DSW DTS profile profile id.	integer	Minimum value: 1 Maximum value: 32	0
step	Set NPU DSW DTS profile step.	integer	Minimum value: 0 Maximum value: 64	0

config dsw-queue-dts-profile

Parameter	Description	Type	Size	Default
iport	Set NPU DSW DTS in port.	option	-	eif0 **
	Option	Description		
	<i>eif0</i>	DSW IPORT EIF0.		
	<i>eif1</i>	DSW IPORT EIF1.		
	<i>eif2</i>	DSW IPORT EIF2.		
	<i>eif3</i>	DSW IPORT EIF3.		
	<i>eif4</i>	DSW IPORT EIF4.		
	<i>eif5</i>	DSW IPORT EIF5.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>elf6</i>	DSW IPORT EIF6.		
	<i>elf7</i>	DSW IPORT EIF7.		
	<i>htx0</i>	DSW IPORT HTX0.		
	<i>htx1</i>	DSW IPORT HTX1.		
	<i>sse0</i>	DSW IPORT SSE0.		
	<i>sse1</i>	DSW IPORT SSE1.		
	<i>sse2</i>	DSW IPORT SSE2.		
	<i>sse3</i>	DSW IPORT SSE3.		
	<i>rlt</i>	DSW IPORT RLT.		
	<i>dfr</i>	DSW IPORT DFR.		
	<i>ipseci</i>	DSW IPORT IPSECI.		
	<i>ipseco</i>	DSW IPORT IPSECO.		
	<i>ipti</i>	DSW IPORT IPTI.		
	<i>ipto</i>	DSW IPORT IPTO.		
	<i>vep0</i>	DSW IPORT VEP0.		
	<i>vep2</i>	DSW IPORT VEP2.		
	<i>vep4</i>	DSW IPORT VEP4.		
	<i>vep6</i>	DSW IPORT VEP6.		
	<i>ivs</i>	DSW IPORT IVS.		
	<i>l2ti1</i>	DSW IPORT L2TI1.		
	<i>l2to</i>	DSW IPORT L2TO.		
	<i>l2ti0</i>	DSW IPORT L2TI0.		
	<i>ple</i>	DSW IPORT PLE.		
	<i>spath</i>	DSW IPORT SPATH.		
	<i>qtm</i>	DSW IPORT QTM.		
name	Name.	string	Maximum length: 35	
oport	Set NPU DSW DTS out port.	option	-	elf0 **

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>elf0</i>	DSW OPORT EIF0.		
	<i>elf1</i>	DSW OPORT EIF1.		
	<i>elf2</i>	DSW OPORT EIF2.		
	<i>elf3</i>	DSW OPORT EIF3.		
	<i>elf4</i>	DSW OPORT EIF4.		
	<i>elf5</i>	DSW OPORT EIF5.		
	<i>elf6</i>	DSW OPORT EIF6.		
	<i>elf7</i>	DSW OPORT EIF7.		
	<i>hrx</i>	DSW OPORT HRX.		
	<i>sse0</i>	DSW OPORT SSE0.		
	<i>sse1</i>	DSW OPORT SSE1.		
	<i>sse2</i>	DSW OPORT SSE2.		
	<i>sse3</i>	DSW OPORT SSE3.		
	<i>rlt</i>	DSW OPORT RLT.		
	<i>dfr</i>	DSW OPORT DFR.		
	<i>ipseci</i>	DSW OPORT IPSECI.		
	<i>ipseco</i>	DSW OPORT IPSECO.		
	<i>ipti</i>	DSW OPORT IPTI.		
	<i>ipto</i>	DSW OPORT IPTO.		
	<i>vep0</i>	DSW OPORT VEP0.		
	<i>vep2</i>	DSW OPORT VEP2.		
	<i>vep4</i>	DSW OPORT VEP4.		
	<i>vep6</i>	DSW OPORT VEP6.		
	<i>ivs</i>	DSW OPORT IVS.		
	<i>l2ti1</i>	DSW OPORT L2TI1.		
	<i>l2to</i>	DSW OPORT L2TO.		
	<i>l2ti0</i>	DSW OPORT L2TI0.		
	<i>ple</i>	DSW OPORT PLE.		
	<i>sync</i>	DSW OPORT SYNK.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>nss</i>	DSW OPORT NSS.		
	<i>tsk</i>	DSW OPORT TSK.		
	<i>qtm</i>	DSW OPORT QTM.		
profile-id	Set NPU DSW DTS profile ID.	integer	Minimum value: 1 Maximum value: 32	0
queue-select	Set NPU DSW DTS queue ID select (0 - reset to default).	integer	Minimum value: 0 Maximum value: 4095	0

** Values may differ between models.

config fp-anomaly

Parameter	Description	Type	Size	Default
gre-csum-err *	Invalid IPv4 GRE checksum anomalies.	option	-	drop
	Option	Description		
	<i>allow</i>	Allow IPv4 invalid GRE checksum.		
	<i>drop</i>	Drop IPv4 invalid GRE checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid GRE checksum to main CPU for processing.		
icmp-csum-err	Invalid IPv4 ICMP checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid ICMP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid ICMP checksum to main CPU for processing.		
icmp-frag *	Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.		
	<i>drop</i>	Drop L3 fragment packet with L4 protocol as ICMP attack.		
	<i>trap-to-host</i>	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.		

Parameter	Description	Type	Size	Default								
icmp-land *	ICMP land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow ICMP land attack to pass.</td></tr><tr><td>drop</td><td>Drop ICMP land attack.</td></tr><tr><td>trap-to-host</td><td>Forward ICMP land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow ICMP land attack to pass.	drop	Drop ICMP land attack.	trap-to-host	Forward ICMP land attack to FortiOS.			
Option	Description											
allow	Allow ICMP land attack to pass.											
drop	Drop ICMP land attack.											
trap-to-host	Forward ICMP land attack to FortiOS.											
ipv4-csum-err	Invalid IPv4 IP checksum anomalies.	option	-	drop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid IP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid IP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid IP checksum.	trap-to-host	Forward IPv4 invalid IP checksum to main CPU for processing.					
Option	Description											
drop	Drop IPv4 invalid IP checksum.											
trap-to-host	Forward IPv4 invalid IP checksum to main CPU for processing.											
ipv4-land *	Land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 land attack to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 land attack.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 land attack to pass.	drop	Drop IPv4 land attack.	trap-to-host	Forward IPv4 land attack to FortiOS.			
Option	Description											
allow	Allow IPv4 land attack to pass.											
drop	Drop IPv4 land attack.											
trap-to-host	Forward IPv4 land attack to FortiOS.											
ipv4-optlsrr *	Loose source record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with loose source record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with loose source record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with loose source record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with loose source record route option to pass.	drop	Drop IPv4 with loose source record route option.	trap-to-host	Forward IPv4 with loose source record route option to FortiOS.			
Option	Description											
allow	Allow IPv4 with loose source record route option to pass.											
drop	Drop IPv4 with loose source record route option.											
trap-to-host	Forward IPv4 with loose source record route option to FortiOS.											
ipv4-optrr *	Record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with record route option to pass.	drop	Drop IPv4 with record route option.	trap-to-host	Forward IPv4 with record route option to FortiOS.			
Option	Description											
allow	Allow IPv4 with record route option to pass.											
drop	Drop IPv4 with record route option.											
trap-to-host	Forward IPv4 with record route option to FortiOS.											
ipv4-optsecurity *	Security option anomalies.	option	-	trap-to-host								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>allow</i>	Allow IPv4 with security option to pass.		
	<i>drop</i>	Drop IPv4 with security option.		
	<i>trap-to-host</i>	Forward IPv4 with security option to FortiOS.		
ipv4-optssrr *	Strict source record route option anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow IPv4 with strict source record route option to pass.		
	<i>drop</i>	Drop IPv4 with strict source record route option.		
	<i>trap-to-host</i>	Forward IPv4 with strict source record route option to FortiOS.		
ipv4-optstream *	Stream option anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow IPv4 with stream option to pass.		
	<i>drop</i>	Drop IPv4 with stream option.		
	<i>trap-to-host</i>	Forward IPv4 with stream option to FortiOS.		
ipv4-opttimestamp *	Timestamp option anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow IPv4 with timestamp option to pass.		
	<i>drop</i>	Drop IPv4 with timestamp option.		
	<i>trap-to-host</i>	Forward IPv4 with timestamp option to FortiOS.		
ipv4-proto-err *	Invalid layer 4 protocol anomalies.	option	-	trap-to-host
	Option Description			
	<i>allow</i>	Allow IPv4 invalid L4 protocol to pass.		
	<i>drop</i>	Drop IPv4 invalid L4 protocol.		
	<i>trap-to-host</i>	Forward IPv4 invalid L4 protocol to FortiOS.		
ipv4-unknopt *	Unknown option anomalies.	option	-	trap-to-host

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv4 with unknown options to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv4 with unknown options.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv4 with unknown options to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv4 with unknown options to pass.	<i>drop</i>	Drop IPv4 with unknown options.	<i>trap-to-host</i>	Forward IPv4 with unknown options to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv4 with unknown options to pass.										
	<i>drop</i>	Drop IPv4 with unknown options.										
<i>trap-to-host</i>	Forward IPv4 with unknown options to FortiOS.											
ipv6-daddr-err *	Destination address as unspecified or loopback address anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with destination address as unspecified or loopback address to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with destination address as unspecified or loopback address.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with destination address as unspecified or loopback address to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with destination address as unspecified or loopback address to pass.	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.	<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 with destination address as unspecified or loopback address to pass.										
	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.										
<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.											
ipv6-land *	Land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 land attack to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 land attack.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 land attack to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 land attack to pass.	<i>drop</i>	Drop IPv6 land attack.	<i>trap-to-host</i>	Forward IPv6 land attack to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 land attack to pass.										
	<i>drop</i>	Drop IPv6 land attack.										
<i>trap-to-host</i>	Forward IPv6 land attack to FortiOS.											
ipv6-optendpid *	End point identification anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with end point identification option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with end point identification option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with end point identification option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with end point identification option to pass.	<i>drop</i>	Drop IPv6 with end point identification option.	<i>trap-to-host</i>	Forward IPv6 with end point identification option to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 with end point identification option to pass.										
	<i>drop</i>	Drop IPv6 with end point identification option.										
<i>trap-to-host</i>	Forward IPv6 with end point identification option to FortiOS.											
ipv6-opthomeaddr *	Home address option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow IPv6 with home address option to pass.</td></tr><tr><td><i>drop</i></td><td>Drop IPv6 with home address option.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward IPv6 with home address option to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow IPv6 with home address option to pass.	<i>drop</i>	Drop IPv6 with home address option.	<i>trap-to-host</i>	Forward IPv6 with home address option to FortiOS.			
	Option	Description										
	<i>allow</i>	Allow IPv6 with home address option to pass.										
	<i>drop</i>	Drop IPv6 with home address option.										
<i>trap-to-host</i>	Forward IPv6 with home address option to FortiOS.											

Parameter	Description	Type	Size	Default								
ipv6-optinvld *	Invalid option anomalies.Invalid option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with invalid option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with invalid option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with invalid option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with invalid option to pass.	drop	Drop IPv6 with invalid option.	trap-to-host	Forward IPv6 with invalid option to FortiOS.			
Option	Description											
allow	Allow IPv6 with invalid option to pass.											
drop	Drop IPv6 with invalid option.											
trap-to-host	Forward IPv6 with invalid option to FortiOS.											
ipv6-optjumbo *	Jumbo options anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with jumbo option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with jumbo option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with jumbo option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with jumbo option to pass.	drop	Drop IPv6 with jumbo option.	trap-to-host	Forward IPv6 with jumbo option to FortiOS.			
Option	Description											
allow	Allow IPv6 with jumbo option to pass.											
drop	Drop IPv6 with jumbo option.											
trap-to-host	Forward IPv6 with jumbo option to FortiOS.											
ipv6-optnsap *	Network service access point address option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with network service access point address option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with network service access point address option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with network service access point address option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with network service access point address option to pass.	drop	Drop IPv6 with network service access point address option.	trap-to-host	Forward IPv6 with network service access point address option to FortiOS.			
Option	Description											
allow	Allow IPv6 with network service access point address option to pass.											
drop	Drop IPv6 with network service access point address option.											
trap-to-host	Forward IPv6 with network service access point address option to FortiOS.											
ipv6-optralert *	Router alert option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with router alert option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with router alert option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with router alert option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with router alert option to pass.	drop	Drop IPv6 with router alert option.	trap-to-host	Forward IPv6 with router alert option to FortiOS.			
Option	Description											
allow	Allow IPv6 with router alert option to pass.											
drop	Drop IPv6 with router alert option.											
trap-to-host	Forward IPv6 with router alert option to FortiOS.											
ipv6-opttunnel *	Tunnel encapsulation limit option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with tunnel encapsulation limit to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with tunnel encapsulation limit.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with tunnel encapsulation limit to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with tunnel encapsulation limit to pass.	drop	Drop IPv6 with tunnel encapsulation limit.	trap-to-host	Forward IPv6 with tunnel encapsulation limit to FortiOS.			
Option	Description											
allow	Allow IPv6 with tunnel encapsulation limit to pass.											
drop	Drop IPv6 with tunnel encapsulation limit.											
trap-to-host	Forward IPv6 with tunnel encapsulation limit to FortiOS.											

Parameter	Description	Type	Size	Default								
ipv6-proto-err *	Layer 4 invalid protocol anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 L4 invalid protocol to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 L4 invalid protocol.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 L4 invalid protocol to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 L4 invalid protocol to pass.	drop	Drop IPv6 L4 invalid protocol.	trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.			
Option	Description											
allow	Allow IPv6 L4 invalid protocol to pass.											
drop	Drop IPv6 L4 invalid protocol.											
trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.											
ipv6-saddr-err *	Source address as multicast anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with source address as multicast to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with source address as multicast.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with source address as multicast to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with source address as multicast to pass.	drop	Drop IPv6 with source address as multicast.	trap-to-host	Forward IPv6 with source address as multicast to FortiOS.			
Option	Description											
allow	Allow IPv6 with source address as multicast to pass.											
drop	Drop IPv6 with source address as multicast.											
trap-to-host	Forward IPv6 with source address as multicast to FortiOS.											
ipv6-unknopt *	Unknown option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with unknown options to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with unknown options.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with unknown options to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with unknown options to pass.	drop	Drop IPv6 with unknown options.	trap-to-host	Forward IPv6 with unknown options to FortiOS.			
Option	Description											
allow	Allow IPv6 with unknown options to pass.											
drop	Drop IPv6 with unknown options.											
trap-to-host	Forward IPv6 with unknown options to FortiOS.											
sctp-csum-err *	Invalid IPv4 SCTP checksum anomalies.	option	-	drop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 invalid SCTP checksum.</td></tr><tr><td>drop</td><td>Drop IPv4 invalid SCTP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid SCTP checksum to main CPU for processing.</td></tr></table>	Option	Description	allow	Allow IPv4 invalid SCTP checksum.	drop	Drop IPv4 invalid SCTP checksum.	trap-to-host	Forward IPv4 invalid SCTP checksum to main CPU for processing.			
Option	Description											
allow	Allow IPv4 invalid SCTP checksum.											
drop	Drop IPv4 invalid SCTP checksum.											
trap-to-host	Forward IPv4 invalid SCTP checksum to main CPU for processing.											
tcp-csum-err	Invalid IPv4 TCP checksum anomalies.	option	-	drop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid TCP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid TCP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid TCP checksum.	trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.					
Option	Description											
drop	Drop IPv4 invalid TCP checksum.											
trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.											
tcp-fin-noack *	TCP SYN flood with FIN flag set without ACK setting anomalies.	option	-	trap-to-host								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow TCP packets with FIN flag set without ack setting to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set without ack setting.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set without ack setting to FortiOS.		
tcp-fin-only *	TCP SYN flood with only FIN flag set anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow TCP packets with FIN flag set only to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set only.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set only to FortiOS.		
tcp-land *	TCP land anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow TCP land attack to pass.		
	<i>drop</i>	Drop TCP land attack.		
	<i>trap-to-host</i>	Forward TCP land attack to FortiOS.		
tcp-no-flag *	TCP SYN flood with no flag set anomalies.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow TCP packets without flag set to pass.		
	<i>drop</i>	Drop TCP packets without flag set.		
	<i>trap-to-host</i>	Forward TCP packets without flag set to FortiOS.		
tcp-syn-data *	TCP SYN flood packets with data anomalies.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow TCP syn packets with data to pass.		
	<i>drop</i>	Drop TCP syn packets with data.		
	<i>trap-to-host</i>	Forward TCP syn packets with data to FortiOS.		
tcp-syn-fin *	TCP SYN flood SYN/FIN flag set anomalies.	option	-	allow

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow TCP packets with syn_fin flag set to pass.		
	<i>drop</i>	Drop TCP packets with syn_fin flag set.		
	<i>trap-to-host</i>	Forward TCP packets with syn_fin flag set to FortiOS.		
tcp-winnuke *	TCP WinNuke anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow TCP packets winnuke attack to pass.		
	<i>drop</i>	Drop TCP packets winnuke attack.		
	<i>trap-to-host</i>	Forward TCP packets winnuke attack to FortiOS.		
udp-csum-err	Invalid IPv4 UDP checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP checksum to main CPU for processing.		
udp-land *	UDP land anomalies.	option	-	trap-to-host
	Option	Description		
	<i>allow</i>	Allow UDP land attack to pass.		
	<i>drop</i>	Drop UDP land attack.		
	<i>trap-to-host</i>	Forward UDP land attack to FortiOS.		
udplite-csum-err *	Invalid IPv4 UDPlite checksum anomalies.	option	-	drop
	Option	Description		
	<i>allow</i>	Allow invalid IPv4 UDPlite checksum.		
	<i>drop</i>	Drop invalid IPv4 UDPlite checksum.		
	<i>trap-to-host</i>	Forward invalid IPv4 UDPlite checksum to main CPU for processing.		

* This parameter may not exist in some models.

config hpe

Parameter	Description	Type	Size	Default
all-protocol	Maximum packet rate of each host queue except high priority traffic(1K - 32M pps, default = 400K pps), set 0 to disable.	integer	Minimum value: 0 Maximum value: 32000000	400000 **
arp-max	Maximum ARP packet rate (1K - 32M pps, default = 5K pps). Entry is valid when ARP is removed from high-priority traffic.	integer	Minimum value: 1000 Maximum value: 32000000	5000
enable-shaper	Enable/Disable NPU Host Protection Engine (HPE) for packet type shaper.	option	-	disable
	Option	Description		
	disable	Disable NPU HPE shaping based on packet type.		
	enable	Enable NPU HPE shaping based on packet type.		
esp-max	Maximum ESP packet rate (1K - 32M pps, default = 5K pps).	integer	Minimum value: 1000 Maximum value: 32000000	5000
high-priority	Maximum packet rate for high priority traffic packets (1K - 32M pps, default = 400K pps).	integer	Minimum value: 1000 Maximum value: 32000000	400000 **
icmp-max	Maximum ICMP packet rate (1K - 32M pps, default = 5K pps).	integer	Minimum value: 1000 Maximum value: 32000000	5000
ip-frag-max	Maximum fragmented IP packet rate (1K - 32M pps, default = 5K pps).	integer	Minimum value: 1000 Maximum value: 32000000	5000

Parameter	Description	Type	Size	Default
ip-others-max	Maximum IP packet rate for other packets (packet types that cannot be set with other options) (1K - 32G pps, default = 5K pps).	integer	Minimum value: 1000 Maximum value: 32000000	5000
l2-others-max	Maximum L2 packet rate for L2 packets that are not ARP packets (1K - 32M pps, default = 5K pps).	integer	Minimum value: 1000 Maximum value: 32000000	5000
sctp-max	Maximum SCTP packet rate (1K - 32M pps, default = 5K pps).	integer	Minimum value: 1000 Maximum value: 32000000	5000
tcp-max	Maximum TCP packet rate (1K - 32M pps, default = 40K pps).	integer	Minimum value: 1000 Maximum value: 32000000	40000
tcpfin-rst-max	Maximum TCP carries FIN or RST flags packet rate (1K - 32M pps, default = 40K pps).	integer	Minimum value: 1000 Maximum value: 32000000	40000
tcpsyn-ack-max	Maximum TCP carries SYN and ACK flags packet rate (1K - 32M pps, default = 40K pps).	integer	Minimum value: 1000 Maximum value: 32000000	40000
tcpsyn-max	Maximum TCP SYN packet rate (1K - 40M pps, default = 32K pps).	integer	Minimum value: 1000 Maximum value: 32000000	40000
udp-max	Maximum UDP packet rate (1K - 32M pps, default = 40K pps).	integer	Minimum value: 1000 Maximum value: 32000000	40000

** Values may differ between models.

config ip-reassembly

Parameter	Description	Type	Size	Default						
max-timeout	Maximum timeout value for IP reassembly (5 us - 600,000,000 us).	integer	Minimum value: 5 Maximum value: 600000000	200000						
min-timeout	Minimum timeout value for IP reassembly (5 us - 600,000,000 us).	integer	Minimum value: 5 Maximum value: 600000000	64						
status	Set IP reassembly processing status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IP reassembly.</td></tr><tr><td><i>enable</i></td><td>Enable IP reassembly.</td></tr></table>				Option	Description	<i>disable</i>	Disable IP reassembly.	<i>enable</i>	Enable IP reassembly.
Option	Description									
<i>disable</i>	Disable IP reassembly.									
<i>enable</i>	Enable IP reassembly.									

config isf-np-queues

Parameter	Description	Type	Size	Default
cos0	CoS profile name for CoS 0.	string	Maximum length: 35	
cos1	CoS profile name for CoS 1.	string	Maximum length: 35	
cos2	CoS profile name for CoS 2.	string	Maximum length: 35	
cos3	CoS profile name for CoS 3.	string	Maximum length: 35	
cos4	CoS profile name for CoS 4.	string	Maximum length: 35	
cos5	CoS profile name for CoS 5.	string	Maximum length: 35	
cos6	CoS profile name for CoS 6.	string	Maximum length: 35	
cos7	CoS profile name for CoS 7.	string	Maximum length: 35	

config ethernet-type

Parameter	Description	Type	Size	Default
name	Ethernet Type Name.	string	Maximum length: 35	
queue	Queue Number.	integer	Minimum value: 0 Maximum value: 11	0
type	Ethernet Type.	ether-type	Not Specified	0
weight	Class Weight.	integer	Minimum value: 0 Maximum value: 15	15

config ip-protocol

Parameter	Description	Type	Size	Default
name	IP Protocol Name.	string	Maximum length: 35	
protocol	IP Protocol.	integer	Minimum value: 0 Maximum value: 255	0
queue	Queue Number.	integer	Minimum value: 0 Maximum value: 11	0
weight	Class Weight.	integer	Minimum value: 0 Maximum value: 15	14

config ip-service

Parameter	Description	Type	Size	Default
dport	Destination port.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
name	IP service name.	string	Maximum length: 35	
protocol	IP protocol.	integer	Minimum value: 0 Maximum value: 255	0
queue	Queue number.	integer	Minimum value: 0 Maximum value: 11	0
sport	Source port.	integer	Minimum value: 0 Maximum value: 65535	0
weight	Class weight.	integer	Minimum value: 0 Maximum value: 15	13

config profile

Parameter	Description	Type	Size	Default
cos0	Queue number of CoS 0.	option	-	queue0
	Option	Description		
	queue0	Queue number 0.		
	queue1	Queue number 1.		
	queue2	Queue number 2.		
	queue3	Queue number 3.		
	queue4	Queue number 4.		
	queue5	Queue number 5.		
	queue6	Queue number 6.		
	queue7	Queue number 7.		
cos1	Queue number of CoS 1.	option	-	queue1

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos2	Queue number of CoS 2.	option	-	queue2
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos3	Queue number of CoS 3.	option	-	queue3
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
cos4	Queue number of CoS 4.	option	-	queue4
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos5	Queue number of CoS 5.	option	-	queue5
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos6	Queue number of CoS 6.	option	-	queue6
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue7	Queue number 7.																		
	Option	Description																					
	queue7	Queue number 7.																					
	cos7	Queue number of CoS 7.	option	-	queue7																		
		<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.			
		Option	Description																				
		queue0	Queue number 0.																				
		queue1	Queue number 1.																				
		queue2	Queue number 2.																				
queue3		Queue number 3.																					
queue4		Queue number 4.																					
queue5		Queue number 5.																					
queue6	Queue number 6.																						
queue7	Queue number 7.																						
dscp0	Queue number of DSCP 0.	option	-	queue0																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.				
	Option	Description																					
	queue0	Queue number 0.																					
	queue1	Queue number 1.																					
	queue2	Queue number 2.																					
	queue3	Queue number 3.																					
	queue4	Queue number 4.																					
	queue5	Queue number 5.																					
queue6	Queue number 6.																						
queue7	Queue number 7.																						
dscp1	Queue number of DSCP 1.	option	-	queue1																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.												
	Option	Description																					
	queue0	Queue number 0.																					
	queue1	Queue number 1.																					
	queue2	Queue number 2.																					
queue3	Queue number 3.																						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp10	Queue number of DSCP 10.	option	-	queue2
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp11	Queue number of DSCP 11.	option	-	queue3
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp12	Queue number of DSCP 12.	option	-	queue4
	Option	Description		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.					
	Option	Description																				
	queue1	Queue number 1.																				
	queue2	Queue number 2.																				
	queue3	Queue number 3.																				
	queue4	Queue number 4.																				
	queue5	Queue number 5.																				
	queue6	Queue number 6.																				
queue7	Queue number 7.																					
dscp13	Queue number of DSCP 13.	option	-	queue5																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.			
	Option	Description																				
	queue0	Queue number 0.																				
	queue1	Queue number 1.																				
	queue2	Queue number 2.																				
	queue3	Queue number 3.																				
	queue4	Queue number 4.																				
	queue5	Queue number 5.																				
queue6	Queue number 6.																					
queue7	Queue number 7.																					
dscp14	Queue number of DSCP 14.	option	-	queue6																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.			
	Option	Description																				
	queue0	Queue number 0.																				
	queue1	Queue number 1.																				
	queue2	Queue number 2.																				
	queue3	Queue number 3.																				
	queue4	Queue number 4.																				
	queue5	Queue number 5.																				
queue6	Queue number 6.																					
queue7	Queue number 7.																					
dscp15	Queue number of DSCP 15.	option	-	queue7																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp16	Queue number of DSCP 16.	option	-	queue0
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp17	Queue number of DSCP 17.	option	-	queue1
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
dscp18	Queue number of DSCP 18.	option	-	queue2
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp19	Queue number of DSCP 19.	option	-	queue3
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp2	Queue number of DSCP 2.	option	-	queue2
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue7</i>	Queue number 7.		
dscp20	Queue number of DSCP 20.	option	-	queue4
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp21	Queue number of DSCP 21.	option	-	queue5
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp22	Queue number of DSCP 22.	option	-	queue6
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp23	Queue number of DSCP 23.	option	-	queue7
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp24	Queue number of DSCP 24.	option	-	queue0
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp25	Queue number of DSCP 25.	option	-	queue1
	Option	Description		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.					
	Option	Description																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
	<i>queue6</i>	Queue number 6.																				
<i>queue7</i>	Queue number 7.																					
dscp26	Queue number of DSCP 26.	option	-	queue2																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
<i>queue6</i>	Queue number 6.																					
<i>queue7</i>	Queue number 7.																					
dscp27	Queue number of DSCP 27.	option	-	queue3																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
<i>queue6</i>	Queue number 6.																					
<i>queue7</i>	Queue number 7.																					
dscp28	Queue number of DSCP 28.	option	-	queue4																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp29	Queue number of DSCP 29.	option	-	queue5
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp3	Queue number of DSCP 3.	option	-	queue3
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
dscp30	Queue number of DSCP 30.	option	-	queue6
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp31	Queue number of DSCP 31.	option	-	queue7
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp32	Queue number of DSCP 32.	option	-	queue0
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue7</i>	Queue number 7.		
dscp33	Queue number of DSCP 33.	option	-	queue1
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp34	Queue number of DSCP 34.	option	-	queue2
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp35	Queue number of DSCP 35.	option	-	queue3
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp36	Queue number of DSCP 36.	option	-	queue4
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp37	Queue number of DSCP 37.	option	-	queue5
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp38	Queue number of DSCP 38.	option	-	queue6
	Option	Description		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp39	Queue number of DSCP 39.	option	-	queue7
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp4	Queue number of DSCP 4.	option	-	queue4
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp40	Queue number of DSCP 40.	option	-	queue0

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp41	Queue number of DSCP 41.	option	-	queue1
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp42	Queue number of DSCP 42.	option	-	queue2
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
dscp43	Queue number of DSCP 43.	option	-	queue3
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp44	Queue number of DSCP 44.	option	-	queue4
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp45	Queue number of DSCP 45.	option	-	queue5
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue7	Queue number 7.																	
	Option	Description																				
	queue7	Queue number 7.																				
	Queue number of DSCP 46.	option	-	queue6																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.			
	Option	Description																				
	queue0	Queue number 0.																				
	queue1	Queue number 1.																				
	queue2	Queue number 2.																				
queue3	Queue number 3.																					
queue4	Queue number 4.																					
queue5	Queue number 5.																					
queue6	Queue number 6.																					
queue7	Queue number 7.																					
Queue number of DSCP 47.	option	-	queue7																			
<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.				
Option	Description																					
queue0	Queue number 0.																					
queue1	Queue number 1.																					
queue2	Queue number 2.																					
queue3	Queue number 3.																					
queue4	Queue number 4.																					
queue5	Queue number 5.																					
queue6	Queue number 6.																					
queue7	Queue number 7.																					
Queue number of DSCP 48.	option	-	queue0																			
<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.												
Option	Description																					
queue0	Queue number 0.																					
queue1	Queue number 1.																					
queue2	Queue number 2.																					
queue3	Queue number 3.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp49	Queue number of DSCP 49.	option	-	queue1
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp5	Queue number of DSCP 5.	option	-	queue5
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp50	Queue number of DSCP 50.	option	-	queue2
	Option	Description		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp51	Queue number of DSCP 51.	option	-	queue3
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp52	Queue number of DSCP 52.	option	-	queue4
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp53	Queue number of DSCP 53.	option	-	queue5

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp54	Queue number of DSCP 54.	option	-	queue6
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp55	Queue number of DSCP 55.	option	-	queue7
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
dscp56	Queue number of DSCP 56.	option	-	queue0
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp57	Queue number of DSCP 57.	option	-	queue1
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp58	Queue number of DSCP 58.	option	-	queue2
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue7	Queue number 7.																	
	Option	Description																				
queue7	Queue number 7.																					
dscp59	Queue number of DSCP 59.	option	-	queue3																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.			
	Option	Description																				
	queue0	Queue number 0.																				
	queue1	Queue number 1.																				
	queue2	Queue number 2.																				
	queue3	Queue number 3.																				
	queue4	Queue number 4.																				
	queue5	Queue number 5.																				
	queue6	Queue number 6.																				
queue7	Queue number 7.																					
dscp6	Queue number of DSCP 6.	option	-	queue6																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.			
	Option	Description																				
	queue0	Queue number 0.																				
	queue1	Queue number 1.																				
	queue2	Queue number 2.																				
	queue3	Queue number 3.																				
	queue4	Queue number 4.																				
	queue5	Queue number 5.																				
	queue6	Queue number 6.																				
queue7	Queue number 7.																					
dscp60	Queue number of DSCP 60.	option	-	queue4																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.											
	Option	Description																				
	queue0	Queue number 0.																				
	queue1	Queue number 1.																				
	queue2	Queue number 2.																				
queue3	Queue number 3.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp61	Queue number of DSCP 61.	option	-	queue5
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp62	Queue number of DSCP 62.	option	-	queue6
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp63	Queue number of DSCP 63.	option	-	queue7
	Option	Description		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp7	Queue number of DSCP 7.	option	-	queue7
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp8	Queue number of DSCP 8.	option	-	queue0
	Option	Description		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp9	Queue number of DSCP 9.	option	-	queue1

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>queue0</td><td>Queue number 0.</td></tr><tr><td>queue1</td><td>Queue number 1.</td></tr><tr><td>queue2</td><td>Queue number 2.</td></tr><tr><td>queue3</td><td>Queue number 3.</td></tr><tr><td>queue4</td><td>Queue number 4.</td></tr><tr><td>queue5</td><td>Queue number 5.</td></tr><tr><td>queue6</td><td>Queue number 6.</td></tr><tr><td>queue7</td><td>Queue number 7.</td></tr></table>	Option	Description	queue0	Queue number 0.	queue1	Queue number 1.	queue2	Queue number 2.	queue3	Queue number 3.	queue4	Queue number 4.	queue5	Queue number 5.	queue6	Queue number 6.	queue7	Queue number 7.			
	Option	Description																				
	queue0	Queue number 0.																				
	queue1	Queue number 1.																				
	queue2	Queue number 2.																				
	queue3	Queue number 3.																				
	queue4	Queue number 4.																				
	queue5	Queue number 5.																				
	queue6	Queue number 6.																				
queue7	Queue number 7.																					
id	Profile ID.	integer	Minimum value: 0 Maximum value: 255	0																		
type	Profile type.	option	-	cos																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cos</td><td>VLAN priority.</td></tr><tr><td>dscp</td><td>IP differentiated services code point.</td></tr></table>	Option	Description	cos	VLAN priority.	dscp	IP differentiated services code point.															
	Option	Description																				
	cos	VLAN priority.																				
dscp	IP differentiated services code point.																					
weight	Class weight.	integer	Minimum value: 0 Maximum value: 15	6																		

config scheduler

Parameter	Description	Type	Size	Default								
mode	Scheduler mode.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Disable QoS on NP7.</td></tr><tr><td><i>priority</i></td><td>Priority Based.</td></tr><tr><td><i>round-robin</i></td><td>Round Robin Scheduler.</td></tr></table>				Option	Description	<i>none</i>	Disable QoS on NP7.	<i>priority</i>	Priority Based.	<i>round-robin</i>	Round Robin Scheduler.
	Option	Description										
	<i>none</i>	Disable QoS on NP7.										
	<i>priority</i>	Priority Based.										
<i>round-robin</i>	Round Robin Scheduler.											
name	Scheduler name.	string	Maximum length: 35									

config npu-tcam

Parameter	Description	Type	Size	Default
name	NPU TCAM policies name.	string	Maximum length: 35	
oid	NPU TCAM OID.	integer	Minimum value: 0 Maximum value: 4095	0
type	TCAM policy type.	option	-	L2_src_tc
	Option	Description		
	L2_src_tc	L2 source port traffic class.		
	L2_tgt_tc	L2 target port traffic class.		
	L2_src_mir	L2 source port mirroring.		
	L2_tgt_mir	L2 target port mirroring.		
	L2_src_act	L2 source port action.		
	L2_tgt_act	L2 target port action.		
	IPv4_src_tc	IPv4 source port traffic class.		
	IPv4_tgt_tc	IPv4 target port traffic class.		
	IPv4_src_mir	IPv4 source port mirroring.		
	IPv4_tgt_mir	IPv4 target port mirroring.		
	IPv4_src_act	IPv4 source port action.		
	IPv4_tgt_act	IPv4 target port action.		
	IPv6_src_tc	IPv6 source port traffic class.		
	IPv6_tgt_tc	IPv6 target port traffic class.		
	IPv6_src_mir	IPv6 source port mirroring.		
	IPv6_tgt_mir	IPv6 target port mirroring.		
	IPv6_src_act	IPv6 source port action.		
IPv6_tgt_act	IPv6 target port action.			
vid	NPU TCAM VID.	integer	Minimum value: 0 Maximum value: 4095	0

config data

Parameter	Description	Type	Size	Default
df	tcam data ip flag df.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ip header df bit.		
	<i>disable</i>	Disable ip header df bit.		
dstip	tcam data dst ipv4 address.	ipv4-address-any	Not Specified	0.0.0.0
dstipv6	tcam data dst ipv6 address.	ipv6-address	Not Specified	::
dstmac	tcam data dst macaddr.	mac-address	Not Specified	00:00:00:00:00:00
dstport	tcam data L4 dst port.	integer	Minimum value: 0 Maximum value: 65535	0
ethertype	tcam data ethertype.	ether-type	Not Specified	0
ext-tag	tcam data extension tag.	option	-	disable
	Option	Description		
	<i>enable</i>	Ftag ext_tag enable.		
	<i>disable</i>	Ftag ext_tag disable.		
frag-off	tcam data ip flag fragment offset.	integer	Minimum value: 0 Maximum value: 31	0
gen-buf-cnt	tcam data gen info buffer count.	integer	Minimum value: 0 Maximum value: 3	0
gen-iv	tcam data gen info iv.	option	-	invalid
	Option	Description		
	<i>valid</i>	gen_i valid.		
	<i>invalid</i>	gen_i valid.		

Parameter	Description	Type	Size	Default						
gen-l3-flags	tcam data gen info L3 flags.	integer	Minimum value: 0 Maximum value: 15	0						
gen-l4-flags	tcam data gen info L4 flags.	integer	Minimum value: 0 Maximum value: 15	0						
gen-pkt-ctrl	tcam data gen info packet control.	integer	Minimum value: 0 Maximum value: 65535	0						
gen-pri	tcam data gen info priority.	integer	Minimum value: 0 Maximum value: 7	0						
gen-pri-v	tcam data gen info priority valid.	option	-	invalid						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>valid</i></td><td>gen_priv valid.</td></tr><tr><td><i>invalid</i></td><td>gen_priv invalid.</td></tr></table>	Option	Description	<i>valid</i>	gen_priv valid.	<i>invalid</i>	gen_priv invalid.			
Option	Description									
<i>valid</i>	gen_priv valid.									
<i>invalid</i>	gen_priv invalid.									
gen-tv	tcam data gen info tv.	option	-	invalid						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>valid</i></td><td>gen_t valid.</td></tr><tr><td><i>invalid</i></td><td>gen_t invalid.</td></tr></table>	Option	Description	<i>valid</i>	gen_t valid.	<i>invalid</i>	gen_t invalid.			
Option	Description									
<i>valid</i>	gen_t valid.									
<i>invalid</i>	gen_t invalid.									
ihl	tcam data ipv4 IHL.	integer	Minimum value: 0 Maximum value: 15	0						
ip4-id	tcam data ipv4 id.	integer	Minimum value: 0 Maximum value: 65535	0						

Parameter	Description	Type	Size	Default
ip6-fl	tcam data ipv6 flow label.	integer	Minimum value: 0 Maximum value: 1048575	0
ipver	tcam data ip header version.	integer	Minimum value: 0 Maximum value: 15	0
l4-wd10	tcam data L4 word10.	integer	Minimum value: 0 Maximum value: 65535	0
l4-wd11	tcam data L4 word11.	integer	Minimum value: 0 Maximum value: 65535	0
l4-wd8	tcam data L4 word8.	integer	Minimum value: 0 Maximum value: 65535	0
l4-wd9	tcam data L4 word9.	integer	Minimum value: 0 Maximum value: 65535	0
mf	tcam data ip flag mf.	option	-	disable
	OptionDescription			
	enableEnable ip header mf bit.			
	disableDisable ip header mf bit.			
protocol	tcam data ip protocol.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default						
slink	tcam data sublink.	integer	Minimum value: 0 Maximum value: 7	0						
smac-change	tcam data source MAC change.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Ftag smac change enable.</td></tr><tr><td>disable</td><td>Ftag smac change disable.</td></tr></table>	Option	Description	enable	Ftag smac change enable.	disable	Ftag smac change disable.			
Option	Description									
enable	Ftag smac change enable.									
disable	Ftag smac change disable.									
sp	tcam data source port.	integer	Minimum value: 0 Maximum value: 4095	0						
src-cfi	tcam data source cfi.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Ftag src_cfi enable.</td></tr><tr><td>disable</td><td>Ftag src_cfi disable.</td></tr></table>	Option	Description	enable	Ftag src_cfi enable.	disable	Ftag src_cfi disable.			
Option	Description									
enable	Ftag src_cfi enable.									
disable	Ftag src_cfi disable.									
src-prio	tcam data source priority.	integer	Minimum value: 0 Maximum value: 7	0						
src-updt	tcam data source update.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Ftag src_updt enable.</td></tr><tr><td>disable</td><td>Ftag src_updt disable.</td></tr></table>	Option	Description	enable	Ftag src_updt enable.	disable	Ftag src_updt disable.			
Option	Description									
enable	Ftag src_updt enable.									
disable	Ftag src_updt disable.									
srcip	tcam data src ipv4 address.	ipv4-address-any	Not Specified	0.0.0.0						
srcipv6	tcam data src ipv6 address.	ipv6-address	Not Specified	::						
srcmac	tcam data src macaddr.	mac-address	Not Specified	00:00:00:00:00:00						

Parameter	Description	Type	Size	Default
srcport	tcam data L4 src port.	integer	Minimum value: 0 Maximum value: 65535	0
svid	tcam data source vid.	integer	Minimum value: 0 Maximum value: 4095	0
tcp-ack	tcam data tcp flag ack.	option	-	disable
	Option	Description		
	enable	Enable tcp header ack bit.		
	disable	Disable tcp header ack bit.		
tcp-cwr	tcam data tcp flag cwr.	option	-	disable
	Option	Description		
	enable	Enable tcp header cwr bit.		
	disable	Disable tcp header cwr bit.		
tcp-ece	tcam data tcp flag ece.	option	-	disable
	Option	Description		
	enable	Enable tcp header ece bit.		
	disable	Disable tcp header ece bit.		
tcp-fin	tcam data tcp flag fin.	option	-	disable
	Option	Description		
	enable	Enable tcp header fin bit.		
	disable	Disable tcp header fin bit.		
tcp-push	tcam data tcp flag push.	option	-	disable
	Option	Description		
	enable	Enable tcp header push bit.		
	disable	Disable tcp header push bit.		
tcp-rst	tcam data tcp flag rst.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable tcp header rst bit.		
	<i>disable</i>	Disable tcp header rst bit.		
tcp-syn	tcam data tcp flag syn.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header syn bit.		
	<i>disable</i>	Disable tcp header syn bit.		
tcp-urg	tcam data tcp flag urg.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header urg bit.		
	<i>disable</i>	Disable tcp header urg bit.		
tgt-cfi	tcam data target cfi.	option	-	disable
	Option	Description		
	<i>enable</i>	Ftag tgt_cfi enable.		
	<i>disable</i>	Ftag tgt_cfi disable.		
tgt-prio	tcam data target priority.	integer	Minimum value: 0 Maximum value: 7	0
tgt-updt	tcam data target port update.	option	-	disable
	Option	Description		
	<i>enable</i>	Ftag tgt update enable.		
	<i>disable</i>	Ftag tgt update disable.		
tgt-v	tcam data target valid.	option	-	invalid
	Option	Description		
	<i>valid</i>	Ftag tgt valid.		
	<i>invalid</i>	Ftag tgt valid.		

Parameter	Description	Type	Size	Default
tos	tcam data ip tos.	integer	Minimum value: 0 Maximum value: 255	0
tp	tcam data target port.	integer	Minimum value: 0 Maximum value: 4095	0
ttl	tcam data ip ttl.	integer	Minimum value: 0 Maximum value: 255	0
tvid	tcam data target vid.	integer	Minimum value: 0 Maximum value: 4095	0
vdiid	tcam data vdom id.	integer	Minimum value: 0 Maximum value: 65535	0

config mask

Parameter	Description	Type	Size	Default						
df	tcam mask ip flag df.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ip header df bit.</td></tr><tr><td><i>disable</i></td><td>Disable ip header df bit.</td></tr></table>				Option	Description	<i>enable</i>	Enable ip header df bit.	<i>disable</i>	Disable ip header df bit.
	Option	Description								
	<i>enable</i>	Enable ip header df bit.								
	<i>disable</i>	Disable ip header df bit.								
dstip	tcam mask dst ipv4 address.	ipv4-address-any	Not Specified	0.0.0.0						
dstipv6	tcam mask dst ipv6 address.	ipv6-address	Not Specified	::						
dstmac	tcam mask dst macaddr.	mac-address	Not Specified	00:00:00:00:00:00						

Parameter	Description	Type	Size	Default
dstport	tcam mask L4 dst port.	integer	Minimum value: 0 Maximum value: 65535	0
ethertype	tcam mask ethertype.	ether-type	Not Specified	0
ext-tag	tcam mask extension tag.	option	-	disable
	Option	Description		
	<i>enable</i>	Ftag ext_tag enable.		
	<i>disable</i>	Ftag ext_tag disable.		
frag-off	tcam data ip flag fragment offset.	integer	Minimum value: 0 Maximum value: 31	0
gen-buf-cnt	tcam mask gen info buffer count.	integer	Minimum value: 0 Maximum value: 3	0
gen-iv	tcam mask gen info iv.	option	-	invalid
	Option	Description		
	<i>valid</i>	gen_i valid.		
	<i>invalid</i>	gen_i valid.		
gen-l3-flags	tcam mask gen info L3 flags.	integer	Minimum value: 0 Maximum value: 15	0
gen-l4-flags	tcam mask gen info L4 flags.	integer	Minimum value: 0 Maximum value: 15	0
gen-pkt-ctrl	tcam mask gen info packet control.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default						
gen-pri	tcam mask gen info priority.	integer	Minimum value: 0 Maximum value: 7	0						
gen-pri-v	tcam mask gen info priority valid.	option	-	invalid						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>valid</i></td><td>gen_priv valid.</td></tr><tr><td><i>invalid</i></td><td>gen_priv invalid.</td></tr></table>	Option	Description	<i>valid</i>	gen_priv valid.	<i>invalid</i>	gen_priv invalid.			
Option	Description									
<i>valid</i>	gen_priv valid.									
<i>invalid</i>	gen_priv invalid.									
gen-tv	tcam mask gen info tv.	option	-	invalid						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>valid</i></td><td>gen_t valid.</td></tr><tr><td><i>invalid</i></td><td>gen_t invalid.</td></tr></table>	Option	Description	<i>valid</i>	gen_t valid.	<i>invalid</i>	gen_t invalid.			
Option	Description									
<i>valid</i>	gen_t valid.									
<i>invalid</i>	gen_t invalid.									
ihl	tcam mask ipv4 IHL.	integer	Minimum value: 0 Maximum value: 15	0						
ip4-id	tcam mask ipv4 id.	integer	Minimum value: 0 Maximum value: 65535	0						
ip6-fl	tcam mask ipv6 flow label.	integer	Minimum value: 0 Maximum value: 1048575	0						
ipver	tcam mask ip header version.	integer	Minimum value: 0 Maximum value: 15	0						
l4-wd10	tcam mask L4 word10.	integer	Minimum value: 0 Maximum value: 65535	0						

Parameter	Description	Type	Size	Default						
l4-wd11	tcam mask L4 word11.	integer	Minimum value: 0 Maximum value: 65535	0						
l4-wd8	tcam mask L4 word8.	integer	Minimum value: 0 Maximum value: 65535	0						
l4-wd9	tcam mask L4 word9.	integer	Minimum value: 0 Maximum value: 65535	0						
mf	tcam mask ip flag mf.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ip header mf bit.</td></tr><tr><td><i>disable</i></td><td>Disable ip header mf bit.</td></tr></table>				Option	Description	<i>enable</i>	Enable ip header mf bit.	<i>disable</i>	Disable ip header mf bit.
	Option	Description								
	<i>enable</i>	Enable ip header mf bit.								
<i>disable</i>	Disable ip header mf bit.									
protocol	tcam mask ip protocol.	integer	Minimum value: 0 Maximum value: 255	0						
slink	tcam mask sublink.	integer	Minimum value: 0 Maximum value: 7	0						
smac-change	tcam mask source MAC change.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Ftag smac change enable.</td></tr><tr><td><i>disable</i></td><td>Ftag smac change disable.</td></tr></table>				Option	Description	<i>enable</i>	Ftag smac change enable.	<i>disable</i>	Ftag smac change disable.
	Option	Description								
	<i>enable</i>	Ftag smac change enable.								
<i>disable</i>	Ftag smac change disable.									
sp	tcam mask source port.	integer	Minimum value: 0 Maximum value: 4095	0						
src-cfi	tcam mask source cfi.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Ftag src_cfi enable.		
	<i>disable</i>	Ftag src_cfi disable.		
src-prio	tcam mask source priority.	integer	Minimum value: 0 Maximum value: 7	0
src-updt	tcam mask source update.	option	-	disable
	Option	Description		
	<i>enable</i>	Ftag src_updt enable.		
	<i>disable</i>	Ftag src_updt disable.		
srcip	tcam mask src ipv4 address.	ipv4-address-any	Not Specified	0.0.0.0
srcipv6	tcam mask src ipv6 address.	ipv6-address	Not Specified	::
srcmac	tcam mask src macaddr.	mac-address	Not Specified	00:00:00:00:00:00
srcport	tcam mask L4 src port.	integer	Minimum value: 0 Maximum value: 65535	0
svid	tcam mask source vid.	integer	Minimum value: 0 Maximum value: 4095	0
tcp-ack	tcam mask tcp flag ack.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header ack bit.		
	<i>disable</i>	Disable tcp header ack bit.		
tcp-cwr	tcam mask tcp flag cwr.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable tcp header cwr bit.		
	<i>disable</i>	Disable tcp header cwr bit.		
tcp-ece	tcam mask tcp flag ece.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header ece bit.		
	<i>disable</i>	Disable tcp header ece bit.		
tcp-fin	tcam mask tcp flag fin.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header fin bit.		
	<i>disable</i>	Disable tcp header fin bit.		
tcp-push	tcam mask tcp flag push.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header push bit.		
	<i>disable</i>	Disable tcp header push bit.		
tcp-rst	tcam mask tcp flag rst.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header rst bit.		
	<i>disable</i>	Disable tcp header rst bit.		
tcp-syn	tcam mask tcp flag syn.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header syn bit.		
	<i>disable</i>	Disable tcp header syn bit.		
tcp-urg	tcam mask tcp flag urg.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tcp header urg bit.		
	<i>disable</i>	Disable tcp header urg bit.		
tgt-cfi	tcam mask target cfi.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Ftag tgt_cfi enable.</td></tr><tr><td><i>disable</i></td><td>Ftag tgt_cfi disable.</td></tr></table>	Option	Description	<i>enable</i>	Ftag tgt_cfi enable.	<i>disable</i>	Ftag tgt_cfi disable.			
	Option	Description								
	<i>enable</i>	Ftag tgt_cfi enable.								
<i>disable</i>	Ftag tgt_cfi disable.									
tgt-prio	tcam mask target priority.	integer	Minimum value: 0 Maximum value: 7	0						
tgt-updt	tcam mask target port update.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Ftag tgt update enable.</td></tr><tr><td><i>disable</i></td><td>Ftag tgt update disable.</td></tr></table>	Option	Description	<i>enable</i>	Ftag tgt update enable.	<i>disable</i>	Ftag tgt update disable.			
	Option	Description								
	<i>enable</i>	Ftag tgt update enable.								
<i>disable</i>	Ftag tgt update disable.									
tgt-v	tcam mask target valid.	option	-	invalid						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>valid</i></td><td>Ftag tgt valid.</td></tr><tr><td><i>invalid</i></td><td>Ftag tgt valid.</td></tr></table>	Option	Description	<i>valid</i>	Ftag tgt valid.	<i>invalid</i>	Ftag tgt valid.			
	Option	Description								
	<i>valid</i>	Ftag tgt valid.								
<i>invalid</i>	Ftag tgt valid.									
tos	tcam mask ip tos.	integer	Minimum value: 0 Maximum value: 255	0						
tp	tcam mask target port.	integer	Minimum value: 0 Maximum value: 4095	0						
ttl	tcam mask ip ttl.	integer	Minimum value: 0 Maximum value: 255	0						
tvid	tcam mask target vid.	integer	Minimum value: 0 Maximum value: 4095	0						
vdid	tcam mask vdom id.	integer	Minimum value: 0 Maximum value: 65535	0						

config mir-act

Parameter	Description	Type	Size	Default
vlif	tcam mirror action vlif.	integer	Minimum value: 0 Maximum value: 16777215	0

config pri-act

Parameter	Description	Type	Size	Default
priority	tcam priority action priority.	integer	Minimum value: 0 Maximum value: 15	0
weight	tcam priority action weight.	integer	Minimum value: 0 Maximum value: 15	0

config sact

Parameter	Description	Type	Size	Default
act	tcam sact act.	integer	Minimum value: 0 Maximum value: 3	0
act-v	Enable to set sact act.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable act.		
	<i>disable</i>	Disable act.		
bmproc	tcam sact bmproc.	integer	Minimum value: 0 Maximum value: 1	0
bmproc-v	Enable to set sact bmproc.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable bmproc.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable bmpoc.		
df-lif	tcam sact df-lif.	integer	Minimum value: 0 Maximum value: 4095	0
df-lif-v	Enable to set sact df-lif.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable df_lif.		
	<i>disable</i>	Disable df_lif.		
dfr	tcam sact dfr.	integer	Minimum value: 0 Maximum value: 1	0
dfr-v	Enable to set sact dfr.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dfr.		
	<i>disable</i>	Disable dfr.		
dmac-skip	tcam sact dmac-skip.	integer	Minimum value: 0 Maximum value: 1	0
dmac-skip-v	Enable to set sact dmac-skip.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dmac_skip.		
	<i>disable</i>	Disable dmac_skip.		
dosen	tcam sact dosen.	integer	Minimum value: 0 Maximum value: 1	0
dosen-v	Enable to set sact dosen.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable dosen.		
	<i>disable</i>	Disable dosen.		
espff-proc	tcam sact espff-proc.	integer	Minimum value: 0 Maximum value: 1	0
espff-proc-v	Enable to set sact espff-proc.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable espff_proc.		
	<i>disable</i>	Disable espff_proc.		
etype-pid	tcam sact etype-pid.	integer	Minimum value: 0 Maximum value: 15	0
etype-pid-v	Enable to set sact etype-pid.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable etype_pid.		
	<i>disable</i>	Disable etype_pid.		
frag-proc	tcam sact frag-proc.	integer	Minimum value: 0 Maximum value: 1	0
frag-proc-v	Enable to set sact frag-proc.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable frag_proc.		
	<i>disable</i>	Disable frag_proc.		
fwd	tcam sact fwd.	integer	Minimum value: 0 Maximum value: 1	0

Parameter	Description	Type	Size	Default						
fwd-lif	tcam sact fwd-lif.	integer	Minimum value: 0 Maximum value: 4095	0						
fwd-lif-v	Enable to set sact fwd-lif.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fwd_lif.</td></tr><tr><td><i>disable</i></td><td>Disable fwd_lif.</td></tr></table>	Option	Description	<i>enable</i>	Enable fwd_lif.	<i>disable</i>	Disable fwd_lif.			
Option	Description									
<i>enable</i>	Enable fwd_lif.									
<i>disable</i>	Disable fwd_lif.									
fwd-tvid	tcam sact fwd-tvid.	integer	Minimum value: 0 Maximum value: 4095	0						
fwd-tvid-v	Enable to set sact fwd-vid.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fwd_tvid.</td></tr><tr><td><i>disable</i></td><td>Disable fwd_tvid.</td></tr></table>	Option	Description	<i>enable</i>	Enable fwd_tvid.	<i>disable</i>	Disable fwd_tvid.			
Option	Description									
<i>enable</i>	Enable fwd_tvid.									
<i>disable</i>	Disable fwd_tvid.									
fwd-v	Enable to set sact fwd.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fwd.</td></tr><tr><td><i>disable</i></td><td>Disable fwd.</td></tr></table>	Option	Description	<i>enable</i>	Enable fwd.	<i>disable</i>	Disable fwd.			
Option	Description									
<i>enable</i>	Enable fwd.									
<i>disable</i>	Disable fwd.									
icpen	tcam sact icpen.	integer	Minimum value: 0 Maximum value: 1	0						
icpen-v	Enable to set sact icpen.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable icpen.</td></tr><tr><td><i>disable</i></td><td>Disable icpen.</td></tr></table>	Option	Description	<i>enable</i>	Enable icpen.	<i>disable</i>	Disable icpen.			
Option	Description									
<i>enable</i>	Enable icpen.									
<i>disable</i>	Disable icpen.									
igmp-mld-snp	tcam sact igmp-mld-snp.	integer	Minimum value: 0 Maximum value: 1	0						

Parameter	Description	Type	Size	Default
igmp-mld-snp-v	Enable to set sact igmp-mld-snp.	option	-	disable
	Option Description			
	<i>enable</i>	Enable igmp_mld_snp.		
	<i>disable</i>	Disable igmp_mld_snp.		
learn	tcam sact learn.	integer	Minimum value: 0 Maximum value: 1	0
learn-v	Enable to set sact learn.	option	-	disable
	Option Description			
	<i>enable</i>	Enable learn.		
	<i>disable</i>	Disable learn.		
m-srh-ctrl	tcam sact m-srh-ctrl.	integer	Minimum value: 0 Maximum value: 1	0
m-srh-ctrl-v	Enable to set sact m-srh-ctrl.	option	-	disable
	Option Description			
	<i>enable</i>	Enable m_srh_ctrl.		
	<i>disable</i>	Disable m_srh_ctrl.		
mac-id	tcam sact mac-id.	integer	Minimum value: 0 Maximum value: 65535	0
mac-id-v	Enable to set sact mac-id.	option	-	disable
	Option Description			
	<i>enable</i>	Enable mac_id.		
	<i>disable</i>	Disable mac_id.		

Parameter	Description	Type	Size	Default						
mss	tcam sact mss.	integer	Minimum value: 0 Maximum value: 16383	0						
mss-v	Enable to set sact mss.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable mss.</td></tr><tr><td><i>disable</i></td><td>Disable mss.</td></tr></table>	Option	Description	<i>enable</i>	Enable mss.	<i>disable</i>	Disable mss.			
Option	Description									
<i>enable</i>	Enable mss.									
<i>disable</i>	Disable mss.									
pleen	tcam sact pleen.	integer	Minimum value: 0 Maximum value: 1	0						
pleen-v	Enable to set sact pleen.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pleen.</td></tr><tr><td><i>disable</i></td><td>Disable pleen.</td></tr></table>	Option	Description	<i>enable</i>	Enable pleen.	<i>disable</i>	Disable pleen.			
Option	Description									
<i>enable</i>	Enable pleen.									
<i>disable</i>	Disable pleen.									
prio-pid	tcam sact prio-pid.	integer	Minimum value: 0 Maximum value: 7	0						
prio-pid-v	Enable to set sact prio-pid.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable prio_pid.</td></tr><tr><td><i>disable</i></td><td>Disable prio_pid.</td></tr></table>	Option	Description	<i>enable</i>	Enable prio_pid.	<i>disable</i>	Disable prio_pid.			
Option	Description									
<i>enable</i>	Enable prio_pid.									
<i>disable</i>	Disable prio_pid.									
promis	tcam sact promis.	integer	Minimum value: 0 Maximum value: 1	0						
promis-v	Enable to set sact promis.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable promis.</td></tr><tr><td><i>disable</i></td><td>Disable promis.</td></tr></table>	Option	Description	<i>enable</i>	Enable promis.	<i>disable</i>	Disable promis.			
Option	Description									
<i>enable</i>	Enable promis.									
<i>disable</i>	Disable promis.									

Parameter	Description	Type	Size	Default						
rfsh	tcam sact rfsh.	integer	Minimum value: 0 Maximum value: 1	0						
rfsh-v	Enable to set sact rfsh.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable rfsh.</td></tr><tr><td>disable</td><td>Disable rfsh.</td></tr></table>	Option	Description	enable	Enable rfsh.	disable	Disable rfsh.			
Option	Description									
enable	Enable rfsh.									
disable	Disable rfsh.									
smac-skip	tcam sact smac-skip.	integer	Minimum value: 0 Maximum value: 1	0						
smac-skip-v	Enable to set sact smac-skip.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable smac_skip.</td></tr><tr><td>disable</td><td>Disable smac_skip.</td></tr></table>	Option	Description	enable	Enable smac_skip.	disable	Disable smac_skip.			
Option	Description									
enable	Enable smac_skip.									
disable	Disable smac_skip.									
tp-smchk-v	Enable to set sact tp mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable tp_smchk.</td></tr><tr><td>disable</td><td>Disable tp_smchk.</td></tr></table>	Option	Description	enable	Enable tp_smchk.	disable	Disable tp_smchk.			
Option	Description									
enable	Enable tp_smchk.									
disable	Disable tp_smchk.									
tp_smchk	tcam sact tp mode.	integer	Minimum value: 0 Maximum value: 1	0						
tpe-id	tcam sact tpe-id.	integer	Minimum value: 0 Maximum value: 16383	0						
tpe-id-v	Enable to set sact tpe-id.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable tpe_id.</td></tr><tr><td>disable</td><td>Disable tpe_id.</td></tr></table>	Option	Description	enable	Enable tpe_id.	disable	Disable tpe_id.			
Option	Description									
enable	Enable tpe_id.									
disable	Disable tpe_id.									

Parameter	Description	Type	Size	Default						
vdm	tcam sact vdm.	integer	Minimum value: 0 Maximum value: 1	0						
vdm-v	Enable to set sact vdm.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable vdm.</td></tr><tr><td>disable</td><td>Disable vdm.</td></tr></table>	Option	Description	enable	Enable vdm.	disable	Disable vdm.			
Option	Description									
enable	Enable vdm.									
disable	Disable vdm.									
vdom-id	tcam sact vdom-id.	integer	Minimum value: 0 Maximum value: 16383	0						
vdom-id-v	Enable to set sact vdom-id.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable vdom_id.</td></tr><tr><td>disable</td><td>Disable vdom_id.</td></tr></table>	Option	Description	enable	Enable vdom_id.	disable	Disable vdom_id.			
Option	Description									
enable	Enable vdom_id.									
disable	Disable vdom_id.									
x-mode	tcam sact x-mode.	integer	Minimum value: 0 Maximum value: 3	0						
x-mode-v	Enable to set sact x-mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable x_mode.</td></tr><tr><td>disable</td><td>Disable x_mode.</td></tr></table>	Option	Description	enable	Enable x_mode.	disable	Disable x_mode.			
Option	Description									
enable	Enable x_mode.									
disable	Disable x_mode.									

config tact

Parameter	Description	Type	Size	Default
act	tcam tact act.	integer	Minimum value: 0 Maximum value: 3	0
act-v	Enable to set tact act.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable act.		
	<i>disable</i>	Disable act.		
fmtuv4-s	tcam tact fmtuv4-s.	integer	Minimum value: 0 Maximum value: 1	0
fmtuv4-s-v	Enable to set tact fmtuv4-s.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable fmtuv4_s.		
	<i>disable</i>	Disable fmtuv4_s.		
fmtuv6-s	tcam tact fmtuv6-s.	integer	Minimum value: 0 Maximum value: 1	0
fmtuv6-s-v	Enable to set tact fmtuv6-s.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable fmtuv6_s.		
	<i>disable</i>	Disable fmtuv6_s.		
Inkid	tcam tact Inkid.	integer	Minimum value: 0 Maximum value: 15	0
Inkid-v	Enable to set tact Inkid.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Inkid.		
	<i>disable</i>	Disable Inkid.		
mac-id	tcam tact mac-id.	integer	Minimum value: 0 Maximum value: 65535	0
mac-id-v	Enable to set tact mac-id.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable mac_id.		
	<i>disable</i>	Disable mac_id.		
mss-t	tcam tact mss.	integer	Minimum value: 0 Maximum value: 16383	0
mss-t-v	Enable to set tact mss.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable mss.		
	<i>disable</i>	Disable mss.		
mtuv4	tcam tact mtuv4.	integer	Minimum value: 0 Maximum value: 16383	0
mtuv4-v	Enable to set tact mtuv4.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable mtuv4.		
	<i>disable</i>	Disable mtuv4.		
mtuv6	tcam tact mtuv6.	integer	Minimum value: 0 Maximum value: 16383	0
mtuv6-v	Enable to set tact mtuv6.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable mtuv6.		
	<i>disable</i>	Disable mtuv6.		
slif-act	tcam tact slif-act.	integer	Minimum value: 0 Maximum value: 3	0

Parameter	Description	Type	Size	Default
slif-act-v	Enable to set tact slif-act.	option	-	disable
	Option Description			
	<i>enable</i>	Enable slif_act.		
	<i>disable</i>	Disable slif_act.		
sublnkid	tcam tact sublnkid.	integer	Minimum value: 0 Maximum value: 511	0
sublnkid-v	Enable to set tact sublnkid.	option	-	disable
	Option Description			
	<i>enable</i>	Enable sublnkid.		
	<i>disable</i>	Disable sublnkid.		
tgvtv-act	tcam tact tgvtv-act.	integer	Minimum value: 0 Maximum value: 1	0
tgvtv-act-v	Enable to set tact tgvtv-act.	option	-	disable
	Option Description			
	<i>enable</i>	Enable tgvtv_act.		
	<i>disable</i>	Disable tgvtv_act.		
tlif-act	tcam tact tlif-act.	integer	Minimum value: 0 Maximum value: 3	0
tlif-act-v	Enable to set tact tlif-act.	option	-	disable
	Option Description			
	<i>enable</i>	Enable tlif_act.		
	<i>disable</i>	Disable tlif_act.		
tpcid	tcam tact tpcid.	integer	Minimum value: 0 Maximum value: 16383	0

Parameter	Description	Type	Size	Default
tpcid-v	Enable to set tact tpcid.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tpcid.		
	<i>disable</i>	Disable tpcid.		
v6fe	tcam tact v6fe.	integer	Minimum value: 0 Maximum value: 1	0
v6fe-v	Enable to set tact v6fe.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable v6fe.		
	<i>disable</i>	Disable v6fe.		
vep-en-v	Enable to set tact vep-en.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable vep_en.		
	<i>disable</i>	Disable vep_en.		
vep-slid	tcam tact vep_slid.	integer	Minimum value: 0 Maximum value: 3	0
vep-slid-v	Enable to set tact vep-slid.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable vep_slid.		
	<i>disable</i>	Disable vep_slid.		
vep_en	tcam tact vep_en.	integer	Minimum value: 0 Maximum value: 1	0
xlt-lif	tcam tact xlt-lif.	integer	Minimum value: 0 Maximum value: 4095	0
xlt-lif-v	Enable to set tact xlt-lif.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable xlt_lif.		
	<i>disable</i>	Disable xlt_lif.		
xlt-vid	tcam tact xlt-vid.	integer	Minimum value: 0 Maximum value: 4095	0
xlt-vid-v	Enable to set tact xlt-vid.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable xlt_vid.		
	<i>disable</i>	Disable xlt_vid.		

config port-cpu-map

Parameter	Description	Type	Size	Default
cpu-core	The CPU core to map to an interface.	string	Maximum length: 31	all
interface	The interface to map to a CPU core.	string	Maximum length: 15	

config port-npu-map

Parameter	Description	Type	Size	Default
interface	Set NPU interface port for NPU group mapping.	string	Maximum length: 15	
npu-group-index	Mapping NPU group index.	integer	Minimum value: 0 Maximum value: 4294967295	0

config port-path-option

Parameter	Description	Type	Size	Default
ports-using-npu <interface-name>	Set ha/aux ports to handle traffic with NPU (otherwise traffic goes to Intel-NIC and then CPU). Available interfaces for NPU path.	string	Maximum length: 15	

config priority-protocol

Parameter	Description	Type	Size	Default						
bfd	Enable/disable NPU BFD priority protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU BFD priority protocol.</td></tr><tr><td><i>disable</i></td><td>Disable NPU BFD priority protocol.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU BFD priority protocol.	<i>disable</i>	Disable NPU BFD priority protocol.			
Option	Description									
<i>enable</i>	Enable NPU BFD priority protocol.									
<i>disable</i>	Disable NPU BFD priority protocol.									
bgp	Enable/disable NPU BGP priority protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU BGP priority protocol.</td></tr><tr><td><i>disable</i></td><td>Disable NPU BGP priority protocol.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU BGP priority protocol.	<i>disable</i>	Disable NPU BGP priority protocol.			
Option	Description									
<i>enable</i>	Enable NPU BGP priority protocol.									
<i>disable</i>	Disable NPU BGP priority protocol.									
slbc	Enable/disable NPU SLBC priority protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU SLBC priority protocol.</td></tr><tr><td><i>disable</i></td><td>Disable NPU SLBC priority protocol.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU SLBC priority protocol.	<i>disable</i>	Disable NPU SLBC priority protocol.			
Option	Description									
<i>enable</i>	Enable NPU SLBC priority protocol.									
<i>disable</i>	Disable NPU SLBC priority protocol.									

config sw-eh-hash

Parameter	Description	Type	Size	Default
computation	Set hashing computation.	option	-	xor16
	Option	Description		
	xor16	Use XOR operator to make 16 bits hash.		
	xor8	Use XOR operator to make 8 bits hash.		
	xor4	Use XOR operator to make 4 bits hash.		
	crc16	Use CRC-16-CCITT polynomial to make 16 bits hash.		
destination-ip-lower-16	Include/exclude destination IP address lower 16 bits.	option	-	include
	Option	Description		
	include	Include destination IP address lower 16 bits.		
	exclude	Exclude destination IP address lower 16 bits.		
destination-ip-upper-16	Include/exclude destination IP address upper 16 bits.	option	-	include

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>include</i>	Include destination IP address upper 16 bits.		
	<i>exclude</i>	Exclude destination IP address upper 16 bits.		
destination-port	Include/exclude destination port if TCP/UDP.	option	-	include
	Option	Description		
	<i>include</i>	Include destination port if TCP/UDP.		
	<i>exclude</i>	Exclude destination port if TCP/UDP.		
ip-protocol	Include/exclude IP protocol.	option	-	include
	Option	Description		
	<i>include</i>	Include IP protocol.		
	<i>exclude</i>	Exclude IP protocol.		
netmask-length	Network mask length.	integer	Minimum value: 17 Maximum value: 32	32
source-ip-lower-16	Include/exclude source IP address lower 16 bits.	option	-	include
	Option	Description		
	<i>include</i>	Include source IP address lower 16 bits.		
	<i>exclude</i>	Exclude source IP address lower 16 bits.		
source-ip-upper-16	Include/exclude source IP address upper 16 bits.	option	-	include
	Option	Description		
	<i>include</i>	Include source IP address upper 16 bits.		
	<i>exclude</i>	Exclude source IP address upper 16 bits.		
source-port	Include/exclude source port if TCP/UDP.	option	-	include
	Option	Description		
	<i>include</i>	Include source port if TCP/UDP.		
	<i>exclude</i>	Exclude source port if TCP/UDP.		

config sw-tr-hash

Parameter	Description	Type	Size	Default						
draco15	Enable/disable DRACO15 hashing.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable using DRACO15 hashing for unicast trunk traffic.</td></tr><tr><td><i>disable</i></td><td>Disable using DRACO15 hashing for unicast trunk traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable using DRACO15 hashing for unicast trunk traffic.	<i>disable</i>	Disable using DRACO15 hashing for unicast trunk traffic.			
Option	Description									
<i>enable</i>	Enable using DRACO15 hashing for unicast trunk traffic.									
<i>disable</i>	Disable using DRACO15 hashing for unicast trunk traffic.									
tcp-udp-port	Include/exclude TCP/UDP source and destination port for unicast trunk traffic.	option	-	exclude						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include TCP/UDP source and destination port for unicast trunk traffic.</td></tr><tr><td><i>exclude</i></td><td>Exclude TCP/UDP source and destination port for unicast trunk traffic.</td></tr></table>	Option	Description	<i>include</i>	Include TCP/UDP source and destination port for unicast trunk traffic.	<i>exclude</i>	Exclude TCP/UDP source and destination port for unicast trunk traffic.			
Option	Description									
<i>include</i>	Include TCP/UDP source and destination port for unicast trunk traffic.									
<i>exclude</i>	Exclude TCP/UDP source and destination port for unicast trunk traffic.									

config system npu-post



This command is available for model(s): FortiGate 1000F, FortiGate 1001F, FortiGate 1800F, FortiGate 1801F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 3200F, FortiGate 3201F, FortiGate 3500F, FortiGate 3501F, FortiGate 3700F, FortiGate 3701F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F.

It is not available for: FortiGate 1000D, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NPU attributes after interface initialization.

```

config system npu-post
    Description: Configure NPU attributes after interface initialization.
    config port-npu-map
        Description: Configure port to NPU group list.
        edit <interface>
            set npu-group <group-name1>, <group-name2>, ...
        next
    end
end

```

config port-npu-map

Parameter	Description	Type	Size	Default
interface	Set NPU interface port for NPU group mapping.	string	Maximum length: 15	
npu-group <group-name>	Mapping NPU group list. NPU group name.	string	Maximum length: 15	

config system npu-setting prp



This command is available for model(s): FortiGate 100F, FortiGate 101F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 60F, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NPU PRP attributes.

```

config system npu-setting prp
    Description: Configure NPU PRP attributes.
    set prp-port-in <interface-name1>, <interface-name2>, ...
    set prp-port-out <interface-name1>, <interface-name2>, ...
end

```

config system npu-setting prp

Parameter	Description	Type	Size	Default
prp-port-in <interface-name>	Ingress port configured to allow the PRP trailer not be stripped off when the PRP packets come in. All of the traffic originating from these ports will always be sent to the host. Physical interface name.	string	Maximum length: 35	
prp-port-out <interface-name>	Egress port configured to allow the PRP trailer not be stripped off when the PRP packets go out. Physical interface name.	string	Maximum length: 35	

config system npu-vlink



This command is available for model(s): FortiGate 1000F, FortiGate 1001F, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 3200F, FortiGate 3201F, FortiGate 3500F, FortiGate 3501F, FortiGate 3700F, FortiGate 3701F, FortiGate 400F, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G.

It is not available for: FortiGate 1000D, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NPU VDOM link.

```

config system npu-vlink
    Description: Configure NPU VDOM link.
    edit <name>
        next
    end

```

config system npu-vlink

Parameter	Description	Type	Size	Default
name	NPU VDOM link name in format npuX_vlink. X means x-th pair of npu-vlink. Maximum 14 characters.	string	Maximum length: 19	

config system ntp

Configure system NTP information.

```

config system ntp
    Description: Configure system NTP information.
    set authentication [enable|disable]
    set interface <interface-name1>, <interface-name2>, ...
    set key {password}
    set key-id {integer}
    set key-type [MD5|SHA1|...]
    config ntpserver
        Description: Configure the FortiGate to connect to any available third-party NTP server.
        edit <id>
            set authentication [enable|disable]
            set interface {string}
            set interface-select-method [auto|sdwan|...]
            set ip-type [IPv6|IPv4|...]
            set key {password}
            set key-id {integer}
            set key-type [MD5|SHA1|...]
            set ntpv3 [enable|disable]
            set server {string}
            set vrf-select {integer}
        next
    end
    set ntpsync [enable|disable]
    set server-mode [enable|disable]
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set syncinterval {integer}
    set type [fortiguard|custom]
end

```


config system ntp

Parameter	Description	Type	Size	Default								
authentication	Enable/disable authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication.</td></tr><tr><td><i>disable</i></td><td>Disable authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable authentication.	<i>disable</i>	Disable authentication.					
Option	Description											
<i>enable</i>	Enable authentication.											
<i>disable</i>	Disable authentication.											
interface <interface-name>	FortiGate interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services. Interface name.	string	Maximum length: 79									
key	Key for authentication.	password	Not Specified									
key-id	Key ID for authentication.	integer	Minimum value: 0 0 Maximum value: 4294967295									
key-type	Key type for authentication (MD5, SHA1, SHA256).	option	-	MD5								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>MD5</i></td><td>Use MD5 to authenticate the message.</td></tr><tr><td><i>SHA1</i></td><td>Use SHA1 to authenticate the message.</td></tr><tr><td><i>SHA256</i></td><td>Use SHA256 to authenticate the message.</td></tr></table>	Option	Description	<i>MD5</i>	Use MD5 to authenticate the message.	<i>SHA1</i>	Use SHA1 to authenticate the message.	<i>SHA256</i>	Use SHA256 to authenticate the message.			
Option	Description											
<i>MD5</i>	Use MD5 to authenticate the message.											
<i>SHA1</i>	Use SHA1 to authenticate the message.											
<i>SHA256</i>	Use SHA256 to authenticate the message.											
ntpsync	Enable/disable setting the FortiGate system time by synchronizing with an NTP Server.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable synchronization with NTP Server.</td></tr><tr><td><i>disable</i></td><td>Disable synchronization with NTP Server.</td></tr></table>	Option	Description	<i>enable</i>	Enable synchronization with NTP Server.	<i>disable</i>	Disable synchronization with NTP Server.					
Option	Description											
<i>enable</i>	Enable synchronization with NTP Server.											
<i>disable</i>	Disable synchronization with NTP Server.											
server-mode	Enable/disable FortiGate NTP Server Mode. Your FortiGate becomes an NTP server for other devices on your network. The FortiGate relays NTP requests to its configured NTP server.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable FortiGate NTP Server Mode.		
	<i>disable</i>	Disable FortiGate NTP Server Mode.		
source-ip	Source IP address for communication to the NTP server.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address for communication to the NTP server.	ipv6-address	Not Specified	::
syncinterval	NTP synchronization interval (1 - 1440 min).	integer	Minimum value: 60 1 Maximum value: 1440	
type	Use the FortiGuard NTP server or any other available NTP Server.	option	-	fortiguard
	Option Description			
	<i>fortiguard</i>	Use the FortiGuard NTP server.		
	<i>custom</i>	Use any other available NTP server.		

config ntpserver

Parameter	Description	Type	Size	Default
authentication	Enable/disable authentication.	option	-	disable
	Option Description			
	<i>enable</i>	Enable authentication.		
	<i>disable</i>	Disable authentication.		
id	NTP server ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option Description			
	<i>auto</i>	Set outgoing interface automatically.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.					
	Option	Description										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
ip-type	Choose to connect to IPv4 or/and IPv6 NTP server.	option	-	Both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>IPv6</i></td><td>Enable look up for IPv6 NTP server.</td></tr><tr><td><i>IPv4</i></td><td>Enable look up for IPv4 NTP server.</td></tr><tr><td><i>Both</i></td><td>Enable look up for both IPv4 and IPv6 NTP server.</td></tr></table>	Option	Description	<i>IPv6</i>	Enable look up for IPv6 NTP server.	<i>IPv4</i>	Enable look up for IPv4 NTP server.	<i>Both</i>	Enable look up for both IPv4 and IPv6 NTP server.			
	Option	Description										
	<i>IPv6</i>	Enable look up for IPv6 NTP server.										
	<i>IPv4</i>	Enable look up for IPv4 NTP server.										
<i>Both</i>	Enable look up for both IPv4 and IPv6 NTP server.											
key	Key for MD5(NTPv3)/SHA1 (NTPv4)/SHA256(NTPv4) authentication.	password	Not Specified									
key-id	Key ID for authentication.	integer	Minimum value: 0 0 Maximum value: 4294967295									
key-type	Select NTP authentication type.	option	-	MD5								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>MD5</i></td><td>Enable MD5(NTPv3) authentication.</td></tr><tr><td><i>SHA1</i></td><td>Enable SHA1(NTPv4) authentication.</td></tr><tr><td><i>SHA256</i></td><td>Enable SHA256(NTPv4) authentication.</td></tr></table>	Option	Description	<i>MD5</i>	Enable MD5(NTPv3) authentication.	<i>SHA1</i>	Enable SHA1(NTPv4) authentication.	<i>SHA256</i>	Enable SHA256(NTPv4) authentication.			
	Option	Description										
	<i>MD5</i>	Enable MD5(NTPv3) authentication.										
	<i>SHA1</i>	Enable SHA1(NTPv4) authentication.										
<i>SHA256</i>	Enable SHA256(NTPv4) authentication.											
ntp3	Enable to use NTPv3 instead of NTPv4.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NTPv3.</td></tr><tr><td><i>disable</i></td><td>Disable NTPv3 (use NTPv4).</td></tr></table>	Option	Description	<i>enable</i>	Enable NTPv3.	<i>disable</i>	Disable NTPv3 (use NTPv4).					
	Option	Description										
	<i>enable</i>	Enable NTPv3.										
<i>disable</i>	Disable NTPv3 (use NTPv4).											
server	IP address or hostname of the NTP Server.	string	Maximum length: 63									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 0 Maximum value: 511									

config system object-tagging

Configure object tagging.

```

config system object-tagging
    Description: Configure object tagging.
    edit <category>
        set address [disable|mandatory|...]
        set color {integer}
        set device [disable|mandatory|...]
        set interface [disable|mandatory|...]
        set multiple [enable|disable]
        set tags <name1>, <name2>, ...
    next
end

```

config system object-tagging

Parameter	Description	Type	Size	Default
address	Address.	option	-	optional
	Option	Description		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
category	Tag Category.	string	Maximum length: 63	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
device	Device.	option	-	optional
	Option	Description		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
interface	Interface.	option	-	optional
	Option	Description		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		

Parameter	Description	Type	Size	Default						
multiple	Allow multiple tag selection.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable multi-tagging.</td></tr><tr><td>disable</td><td>Disable multi-tagging.</td></tr></table>				Option	Description	enable	Enable multi-tagging.	disable	Disable multi-tagging.
	Option	Description								
	enable	Enable multi-tagging.								
	disable	Disable multi-tagging.								
tags <name>	Tags. Tag name.	string	Maximum length: 79							

config system password-policy

Configure password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.

```

config system password-policy
    Description: Configure password policy for locally defined administrator passwords and IPsec
VPN pre-shared keys.
    set apply-to {option1}, {option2}, ...
    set expire-day {integer}
    set expire-status [enable|disable]
    set login-lockout-upon-weaker-encryption [enable|disable]
    set min-lower-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-upper-case-letter {integer}
    set minimum-length {integer}
    set reuse-password [enable|disable]
    set reuse-password-limit {integer}
    set status [enable|disable]
end

```

config system password-policy

Parameter	Description	Type	Size	Default						
apply-to	Apply password policy to administrator passwords or IPsec pre-shared keys or both. Separate entries with a space.	option	-	admin-password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>admin-password</i></td><td>Apply to administrator passwords.</td></tr><tr><td><i>ipsec-preshared-key</i></td><td>Apply to IPsec pre-shared keys.</td></tr></table>				Option	Description	<i>admin-password</i>	Apply to administrator passwords.	<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.
Option	Description									
<i>admin-password</i>	Apply to administrator passwords.									
<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.									

Parameter	Description	Type	Size	Default						
expire-day	Number of days after which passwords expire (1 - 999 days, default = 90).	integer	Minimum value: 1 Maximum value: 999	90						
expire-status	Enable/disable password expiration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Passwords expire after expire-day days.</td></tr><tr><td><i>disable</i></td><td>Passwords do not expire.</td></tr></table>	Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.			
Option	Description									
<i>enable</i>	Passwords expire after expire-day days.									
<i>disable</i>	Passwords do not expire.									
login-lockout-upon-weaker-encryption	Enable/disable administrative user login lockout upon downgrade (default = disable). If enabled, changing the FortiOS firmware to a version where safer passwords are unsupported will lock out administrative users.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable administrative user login lockout upon downgrade.</td></tr><tr><td><i>disable</i></td><td>Disable administrative user login lockout upon downgrade.</td></tr></table>	Option	Description	<i>enable</i>	Enable administrative user login lockout upon downgrade.	<i>disable</i>	Disable administrative user login lockout upon downgrade.			
Option	Description									
<i>enable</i>	Enable administrative user login lockout upon downgrade.									
<i>disable</i>	Disable administrative user login lockout upon downgrade.									
min-lower-case-letter	Minimum number of lowercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
minimum-length	Minimum password length (8 - 128, default = 8).	integer	Minimum value: 8 Maximum value: 128	8						

Parameter	Description	Type	Size	Default						
reuse-password	Enable/disable reuse of password.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Administrators are allowed to reuse the same password up to a limit.</td></tr><tr><td>disable</td><td>Administrators must create a new password.</td></tr></table>				Option	Description	enable	Administrators are allowed to reuse the same password up to a limit.	disable	Administrators must create a new password.
Option	Description									
enable	Administrators are allowed to reuse the same password up to a limit.									
disable	Administrators must create a new password.									
reuse-password-limit	Number of times passwords can be reused (0 - 20, default = 0. If set to 0, can reuse password an unlimited number of times.).	integer	Minimum value: 0 Maximum value: 20	0						
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable password policy.</td></tr><tr><td>disable</td><td>Disable password policy.</td></tr></table>				Option	Description	enable	Enable password policy.	disable	Disable password policy.
Option	Description									
enable	Enable password policy.									
disable	Disable password policy.									

config system password-policy-guest-admin

Configure the password policy for guest administrators.

```

config system password-policy-guest-admin
    Description: Configure the password policy for guest administrators.
    set apply-to {option1}, {option2}, ...
    set expire-day {integer}
    set expire-status [enable|disable]
    set min-lower-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-upper-case-letter {integer}
    set minimum-length {integer}
    set reuse-password [enable|disable]
    set reuse-password-limit {integer}
    set status [enable|disable]
end

```

config system password-policy-guest-admin

Parameter	Description	Type	Size	Default						
apply-to	Guest administrator to which this password policy applies.	option	-	guest-admin-password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>guest-admin-password</td><td>Apply to guest administrator password.</td></tr></table>	Option	Description	guest-admin-password	Apply to guest administrator password.					
Option	Description									
guest-admin-password	Apply to guest administrator password.									
expire-day	Number of days after which passwords expire (1 - 999 days, default = 90).	integer	Minimum value: 1 Maximum value: 999	90						
expire-status	Enable/disable password expiration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Passwords expire after expire-day days.</td></tr><tr><td>disable</td><td>Passwords do not expire.</td></tr></table>	Option	Description	enable	Passwords expire after expire-day days.	disable	Passwords do not expire.			
Option	Description									
enable	Passwords expire after expire-day days.									
disable	Passwords do not expire.									
min-lower-case-letter	Minimum number of lowercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
minimum-length	Minimum password length (8 - 128, default = 8).	integer	Minimum value: 8 Maximum value: 128	8						
reuse-password	Enable/disable reuse of password.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Administrators are allowed to reuse the same password up to a limit.		
	<i>disable</i>	Administrators must create a new password.		
reuse-password-limit	Number of times passwords can be reused (0 - 20, default = 0. If set to 0, can reuse password an unlimited number of times.).	integer	Minimum value: 0 Maximum value: 20	0
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable password policy.		
	<i>disable</i>	Disable password policy.		

config system pcg-server

Configure PCP server information.

```

config system pcg-server
  Description: Configure PCP server information.
  config pools
    Description: Configure PCP pools.
    edit <name>
      set allow-opcode {option1}, {option2}, ...
      set announcement-count {integer}
      set arp-reply [disable|enable]
      set client-mapping-limit {integer}
      set client-subnet <subnet1>, <subnet2>, ...
      set description {string}
      set ext-intf {string}
      set extip {user}
      set extport {user}
      set id {integer}
      set intl-intf <interface-name1>, <interface-name2>, ...
      set mapping-filter-limit {integer}
      set maximal-lifetime {integer}
      set minimal-lifetime {integer}
      set multicast-announcement [enable|disable]
      set recycle-delay {integer}
      set third-party [allow|disallow]
      set third-party-subnet <subnet1>, <subnet2>, ...
    next
  next

```

```

end
set status [enable|disable]
end

```

config system pcp-server

Parameter	Description	Type	Size	Default
status	Enable/disable PCP server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PCP Server.		
	<i>disable</i>	Disable PCP Server.		

config pools

Parameter	Description	Type	Size	Default
allow-opcode	Allowed PCP opcode.	option	-	map peer announce
	Option	Description		
	<i>map</i>	Allow opcode MAP.		
	<i>peer</i>	Allow opcode PEER.		
	<i>announce</i>	Allow opcode ANNOUNCE.		
announcement-count	Number of multicast announcements.	integer	Minimum value: 3 3 Maximum value: 10	
arp-reply	Enable to respond to ARP requests for external IP (default = enable).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable ARP reply.		
	<i>enable</i>	Enable ARP reply.		
client-mapping-limit	Mapping limit per client (0 - 65535, default = 0, 0 = unlimited).	integer	Minimum value: 0 0 Maximum value: 65535	
client-subnet <subnet>	Subnets from which PCP requests are accepted. Client subnets.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
description	Description.	string	Maximum length: 127							
ext-intf	External interface name.	string	Maximum length: 35							
extip	IP address or address range on the external interface that you want to map to an address on the internal network.	user	Not Specified							
extport	Incoming port number range that you want to map to a port number on the internal network.	user	Not Specified							
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
intl-intf <interface-name>	Internal interface name. Interface name.	string	Maximum length: 79							
mapping-filter-limit	Filter limit per mapping (0 - 5, default = 1).	integer	Minimum value: 1 0 Maximum value: 5							
maximal-lifetime	Maximal lifetime of a PCP mapping in seconds (3600 - 604800, default = 86400).	integer	Minimum value: 3600 Maximum value: 604800	86400						
minimal-lifetime	Minimal lifetime of a PCP mapping in seconds (60 - 300, default = 120).	integer	Minimum value: 60 Maximum value: 300	120						
multicast-announcement	Enable/disable multicast announcements.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable multicast announcements.</td></tr><tr><td>disable</td><td>Disable multicast announcements.</td></tr></table>				Option	Description	enable	Enable multicast announcements.	disable	Disable multicast announcements.
Option	Description									
enable	Enable multicast announcements.									
disable	Disable multicast announcements.									
name	PCP pool name.	string	Maximum length: 79							
recycle-delay	Minimum delay (in seconds) the PCP Server will wait before recycling mappings that have expired (0 - 3600, default = 0).	integer	Minimum value: 0 0 Maximum value: 3600							
third-party	Allow/disallow third party option.	option	-	disallow						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow third party option.		
	<i>disallow</i>	Disallow third party option.		
third-party-subnet <subnet>	Subnets from which third party requests are accepted. Third party subnets.	string	Maximum length: 79	

config system physical-switch



This command is available for model(s): FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 200F, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3200F, FortiGate 3201F, FortiGate 3500F, FortiGate 3501F, FortiGate 3700F, FortiGate 3701F, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

Configure physical switches.

```
config system physical-switch
  Description: Configure physical switches.
  edit <name>
    set age-enable [enable|disable]
    set age-val {integer}
  next
end
```

config system physical-switch

Parameter	Description	Type	Size	Default						
age-enable	Enable/disable layer 2 age timer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable layer 2 ageing timer.</td></tr><tr><td><i>disable</i></td><td>Disable layer 2 ageing timer.</td></tr></table>				Option	Description	<i>enable</i>	Enable layer 2 ageing timer.	<i>disable</i>	Disable layer 2 ageing timer.
	Option	Description								
	<i>enable</i>	Enable layer 2 ageing timer.								
<i>disable</i>	Disable layer 2 ageing timer.									
age-val	Layer 2 table age timer value.	integer	Minimum value: 0 Maximum value: 4294967295	3158067						
name	Name.	string	Maximum length: 15							

config system pppoe-interface

Configure the PPPoE interfaces.

```
config system pppoe-interface
  Description: Configure the PPPoE interfaces.
  edit <name>
    set ac-name {string}
    set auth-type [auto|pap|...]
    set device {string}
    set dial-on-demand [enable|disable]
    set disc-retry-timeout {integer}
    set idle-timeout {integer}
    set ipunnumbered {ipv4-address}
    set ipv6 [enable|disable]
    set lcp-echo-interval {integer}
    set lcp-max-echo-fails {integer}
    set padt-retry-timeout {integer}
    set password {password}
    set pppoe-egress-cos [cos0|cos1|...]
    set pppoe-unnumbered-negotiate [enable|disable]
    set service-name {string}
    set username {string}
  next
end
```

config system pppoe-interface

Parameter	Description	Type	Size	Default												
ac-name	PPPoE AC name.	string	Maximum length: 63													
auth-type	PPP authentication type to use.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Automatically choose the authentication method.</td></tr><tr><td>pap</td><td>PAP authentication.</td></tr><tr><td>chap</td><td>CHAP authentication.</td></tr><tr><td>mschapv1</td><td>MS-CHAPv1 authentication.</td></tr><tr><td>mschapv2</td><td>MS-CHAPv2 authentication.</td></tr></table>	Option	Description	auto	Automatically choose the authentication method.	pap	PAP authentication.	chap	CHAP authentication.	mschapv1	MS-CHAPv1 authentication.	mschapv2	MS-CHAPv2 authentication.			
Option	Description															
auto	Automatically choose the authentication method.															
pap	PAP authentication.															
chap	CHAP authentication.															
mschapv1	MS-CHAPv1 authentication.															
mschapv2	MS-CHAPv2 authentication.															
device	Name for the physical interface.	string	Maximum length: 15													
dial-on-demand	Enable/disable dial on demand to dial the PPPoE interface when packets are routed to the PPPoE interface.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dial on demand.</td></tr><tr><td>disable</td><td>Disable dial on demand.</td></tr></table>	Option	Description	enable	Enable dial on demand.	disable	Disable dial on demand.									
Option	Description															
enable	Enable dial on demand.															
disable	Disable dial on demand.															
disc-retry-timeout	PPPoE discovery init timeout value in (0-4294967295 sec).	integer	Minimum value: 1 0 Maximum value: 4294967295													
idle-timeout	PPPoE auto disconnect after idle timeout (0-4294967295 sec).	integer	Minimum value: 0 0 Maximum value: 4294967295													
ipunnumbered	PPPoE unnumbered IP.	ipv4-address	Not Specified	0.0.0.0												
ipv6	Enable/disable IPv6 Control Protocol (IPv6CP).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPv6CP.</td></tr><tr><td>disable</td><td>Disable IPv6CP.</td></tr></table>	Option	Description	enable	Enable IPv6CP.	disable	Disable IPv6CP.									
Option	Description															
enable	Enable IPv6CP.															
disable	Disable IPv6CP.															

Parameter	Description	Type	Size	Default																		
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 5 0 Maximum value: 32767																			
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 3 0 Maximum value: 32767																			
name	Name of the PPPoE interface.	string	Maximum length: 15																			
padt-retry-timeout	PPPoE terminate timeout value in (0-4294967295 sec).	integer	Minimum value: 1 0 Maximum value: 4294967295																			
password	Enter the password.	password	Not Specified																			
pppoe-egress-cos	CoS in VLAN tag for outgoing PPPoE/PPP packets.	option	-	cos0																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cos0</td><td>CoS 0.</td></tr><tr><td>cos1</td><td>CoS 1.</td></tr><tr><td>cos2</td><td>CoS 2.</td></tr><tr><td>cos3</td><td>CoS 3.</td></tr><tr><td>cos4</td><td>CoS 4.</td></tr><tr><td>cos5</td><td>CoS 5.</td></tr><tr><td>cos6</td><td>CoS 6.</td></tr><tr><td>cos7</td><td>CoS 7.</td></tr></table>				Option	Description	cos0	CoS 0.	cos1	CoS 1.	cos2	CoS 2.	cos3	CoS 3.	cos4	CoS 4.	cos5	CoS 5.	cos6	CoS 6.	cos7	CoS 7.
Option	Description																					
cos0	CoS 0.																					
cos1	CoS 1.																					
cos2	CoS 2.																					
cos3	CoS 3.																					
cos4	CoS 4.																					
cos5	CoS 5.																					
cos6	CoS 6.																					
cos7	CoS 7.																					
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable PPPoE unnumbered negotiation.</td></tr><tr><td>disable</td><td>Disable PPPoE unnumbered negotiation.</td></tr></table>				Option	Description	enable	Enable PPPoE unnumbered negotiation.	disable	Disable PPPoE unnumbered negotiation.												
Option	Description																					
enable	Enable PPPoE unnumbered negotiation.																					
disable	Disable PPPoE unnumbered negotiation.																					
service-name	PPPoE service name.	string	Maximum length: 63																			
username	User name.	string	Maximum length: 64																			

config system probe-response

Configure system probe response.

```
config system probe-response
  Description: Configure system probe response.
  set http-probe-value {string}
  set mode [none|http-probe|...]
  set password {password}
  set port {integer}
  set security-mode [none|authentication]
  set timeout {integer}
  set ttl-mode [reinit|decrease|...]
end
```

config system probe-response

Parameter	Description	Type	Size	Default
http-probe-value	Value to respond to the monitoring server.	string	Maximum length: 1024	OK
mode	SLA response mode.	option	-	none
	Option	Description		
	<i>none</i>	Disable probe.		
	<i>http-probe</i>	HTTP probe.		
	<i>twamp</i>	Two way active measurement protocol.		
password	TWAMP responder password in authentication mode.	password	Not Specified	
port	Port number to response.	integer	Minimum value: 1 Maximum value: 65535	8008
security-mode	TWAMP responder security mode.	option	-	none
	Option	Description		
	<i>none</i>	Unauthenticated mode.		
	<i>authentication</i>	Authenticated mode.		

Parameter	Description	Type	Size	Default								
timeout	An inactivity timer for a twamp test session.	integer	Minimum value: 10 Maximum value: 3600	300								
tll-mode	Mode for TWAMP packet TTL modification.	option	-	retain								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reinit</i></td><td>Reinitialize TTL.</td></tr><tr><td><i>decrease</i></td><td>Decrease TTL.</td></tr><tr><td><i>retain</i></td><td>Retain TTL.</td></tr></table>				Option	Description	<i>reinit</i>	Reinitialize TTL.	<i>decrease</i>	Decrease TTL.	<i>retain</i>	Retain TTL.
Option	Description											
<i>reinit</i>	Reinitialize TTL.											
<i>decrease</i>	Decrease TTL.											
<i>retain</i>	Retain TTL.											

config system proxy-arp

Configure proxy-ARP.

```

config system proxy-arp
  Description: Configure proxy-ARP.
  edit <id>
    set end-ip {ipv4-address}
    set interface {string}
    set ip {ipv4-address}
  next
end

```

config system proxy-arp

Parameter	Description	Type	Size	Default
end-ip	End IP of IP range to be proxied.	ipv4-address	Not Specified	0.0.0.0
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface acting proxy-ARP.	string	Maximum length: 15	
ip	IP address or start IP to be proxied.	ipv4-address	Not Specified	0.0.0.0

config system ptp

Configure system PTP information.

```
config system ptp
  Description: Configure system PTP information.
  set delay-mechanism [E2E|P2P]
  set interface {string}
  set mode [multicast|hybrid]
  set request-interval {integer}
  config server-interface
    Description: FortiGate interface(s) with PTP server mode enabled. Devices on your network
    can contact these interfaces for PTP services.
    edit <id>
      set delay-mechanism [E2E|P2P]
      set server-interface-name {string}
    next
  end
  set server-mode [enable|disable]
  set status [enable|disable]
end
```

config system ptp

Parameter	Description	Type	Size	Default						
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>E2E</td><td>End to end delay detection.</td></tr><tr><td>P2P</td><td>Peer to peer delay detection.</td></tr></table>	Option	Description	E2E	End to end delay detection.	P2P	Peer to peer delay detection.			
Option	Description									
E2E	End to end delay detection.									
P2P	Peer to peer delay detection.									
interface	PTP client will reply through this interface.	string	Maximum length: 15							
mode	Multicast transmission or hybrid transmission.	option	-	multicast						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>multicast</td><td>Send PTP packets with multicast.</td></tr><tr><td>hybrid</td><td>Send PTP packets with unicast and multicast.</td></tr></table>	Option	Description	multicast	Send PTP packets with multicast.	hybrid	Send PTP packets with unicast and multicast.			
Option	Description									
multicast	Send PTP packets with multicast.									
hybrid	Send PTP packets with unicast and multicast.									
request-interval	The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.	integer	Minimum value: 1 Maximum value: 6	1						

Parameter	Description	Type	Size	Default						
server-mode	Enable/disable FortiGate PTP server mode. Your FortiGate becomes an PTP server for other devices on your network.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGate PTP server mode.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGate PTP server mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGate PTP server mode.	<i>disable</i>	Disable FortiGate PTP server mode.			
Option	Description									
<i>enable</i>	Enable FortiGate PTP server mode.									
<i>disable</i>	Disable FortiGate PTP server mode.									
status	Enable/disable setting the FortiGate system time by synchronizing with an PTP Server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable synchronization with PTP Server.</td></tr><tr><td><i>disable</i></td><td>Disable synchronization with PTP Server.</td></tr></table>	Option	Description	<i>enable</i>	Enable synchronization with PTP Server.	<i>disable</i>	Disable synchronization with PTP Server.			
Option	Description									
<i>enable</i>	Enable synchronization with PTP Server.									
<i>disable</i>	Disable synchronization with PTP Server.									

config server-interface

Parameter	Description	Type	Size	Default
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E
	Option	Description		
	E2E	End to end delay detection.		
	P2P	Peer to peer delay detection.		
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
server-interface-name	Interface name.	string	Maximum length: 15	

config system replacemsg admin

Replacement messages. Read-only.

```
config system replacemsg admin
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
```

```

        set format [none|text|...]
        set header [none|http|...]
    next
end

```

config system replacemsg admin

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg alertmail

Replacement messages. Read-only.

```

config system replacemsg alertmail
    Description: Replacement messages. Read-only.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end

```

config system replacemsg alertmail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg auth

Replacement messages. Read-only.

```
config system replacemsg auth
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg auth

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg automation

Replacement messages. Read-only.

```
config system replacemsg automation
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg automation

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg custom-message

Replacement messages. Read-only.

```
config system replacemsg custom-message
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg custom-message

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg fortiguard-wf

Replacement messages. Read-only.

```
config system replacemsg fortiguard-wf
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```


config system replacemsg fortiguard-wf

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg ftp



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Replacement messages. Read-only.

```
config system replacemsg ftp
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg ftp

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg http

Replacement messages. Read-only.

```

config system replacemsg http
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end

```

config system replacemsg http

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg icap



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Replacement messages. Read-only.

```

config system replacemsg icap
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end

```

config system replacemsg icap

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg mail

Replacement messages. Read-only.

```

config system replacemsg mail
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end

```

```
next
end
```

config system replacemsg mail

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></table>	Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.			
	Option	Description										
	<i>none</i>	No format type.										
	<i>text</i>	Text format.										
<i>html</i>	HTML format.											
header	Header flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

config system replacemsg nac-quar

Replacement messages. Read-only.

```
config system replacemsg nac-quar
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg nac-quar

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg spam

Replacement messages. Read-only.

```
config system replacemsg spam
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg spam

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg sslvpn

Replacement messages. Read-only.

```
config system replacemsg sslvpn
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```


config system replacemsg sslvpn

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg traffic-quota

Replacement messages. Read-only.

```
config system replacemsg traffic-quota
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg traffic-quota

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg utm

Replacement messages. Read-only.

```
config system replacemsg utm
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg utm

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg webproxy



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Replacement messages. Read-only.

```
config system replacemsg webproxy
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg webproxy

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg-group

Configure replacement message groups.

```

config system replacemsg-group
  Description: Configure replacement message groups.
  edit <name>
    config admin
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
  config alertmail
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set format [none|text|...]
      set header [none|http|...]
    next
  end
  config auth
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set format [none|text|...]
      set header [none|http|...]
  
```

```

        next
    end
    config automation
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    set comment {var-string}
    config custom-message
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    config fortiguard-wf
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    config ftp
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    set group-type [default|utm|...]
    config http
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    config icap
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
end

```

```

config mail
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config nac-quar
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config spam
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config sslvpn
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config traffic-quota
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config utm
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config webproxy
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}

```

```

        set format [none|text|...]
        set header [none|http|...]
    next
end
next
end

```

config system replacemsg-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
group-type	Group type.	option	-	default
	Option	Description		
	<i>default</i>	Per-vdom replacement messages.		
	<i>utm</i>	For use with UTM settings in firewall policies.		
	<i>auth</i>	For use with authentication pages in firewall policies.		
name	Group name.	string	Maximum length: 35	

config admin

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></table>				Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.
	Option	Description										
	<i>none</i>	No format type.										
	<i>text</i>	Text format.										
<i>html</i>	HTML format.											
header	Header flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP		
	Option	Description										
	<i>none</i>	No header type.										
<i>http</i>	HTTP											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config alertmail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config auth

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config automation

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config custom-message

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config fortiguard-wf

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config ftp

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config http

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config icap

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config mail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config nac-quar

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config spam

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config sslvpn

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config traffic-quota

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config utm

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config webproxy

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg-image

Configure replacement message images.

```
config system replacemsg-image
  Description: Configure replacement message images.
  edit <name>
    set image-base64 {var-string}
    set image-type [gif|jpg|...]
  next
end
```

config system replacemsg-image

Parameter	Description	Type	Size	Default
image-base64	Image data.	var-string	Maximum length: 32768	
image-type	Image type.	option	-	png
	Option	Description		
	<i>gif</i>	GIF image.		
	<i>jpg</i>	JPEG image.		
	<i>tiff</i>	TIFF image.		
	<i>png</i>	PNG image.		
name	Image name.	string	Maximum length: 23	

config system resource-limits

Configure resource limits.

```

config system resource-limits
  Description: Configure resource limits.
  set custom-service {integer}
  set dialup-tunnel {integer}
  set firewall-address {integer}
  set firewall-addrgrp {integer}
  set firewall-policy {integer}
  set ipsec-phase1 {integer}
  set ipsec-phase1-interface {integer}
  set ipsec-phase2 {integer}
  set ipsec-phase2-interface {integer}
  set log-disk-quota {integer}
  set onetime-schedule {integer}
  set proxy {integer}
  set recurring-schedule {integer}
  set service-group {integer}
  set session {integer}
  set sslvpn {integer}
  set user {integer}
  set user-group {integer}
end

```

config system resource-limits

Parameter	Description	Type	Size	Default
custom-service	Maximum number of firewall custom services.	integer	Minimum value: 0 Maximum value: 4294967295	
dialup-tunnel	Maximum number of dial-up tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-address	Maximum number of firewall addresses (IPv4, IPv6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-addrgrp	Maximum number of firewall address groups (IPv4, IPv6).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-policy	Maximum number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
ipsec-phase1	Maximum number of VPN IPsec phase1 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase1-interface	Maximum number of VPN IPsec phase1 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase2	Maximum number of VPN IPsec phase2 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase2-interface	Maximum number of VPN IPsec phase2 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
log-disk-quota	Log disk quota in megabytes (MB).	integer	Minimum value: 0 0 Maximum value: 4294967295 **	
onetime-schedule	Maximum number of firewall one-time schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
proxy *	Maximum number of concurrent proxy users.	integer	Minimum value: 0 Maximum value: 4294967295	
recurring-schedule	Maximum number of firewall recurring schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
service-group	Maximum number of firewall service groups.	integer	Minimum value: 0 Maximum value: 4294967295	
session	Maximum number of sessions.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
sslvpn *	Maximum number of Agentless VPN.	integer	Minimum value: 0 Maximum value: 4294967295	
user	Maximum number of local users.	integer	Minimum value: 0 Maximum value: 4294967295	
user-group	Maximum number of user groups.	integer	Minimum value: 0 Maximum value: 4294967295	

** Values may differ between models.

* This parameter may not exist in some models.

config system saml

Global settings for SAML authentication.

```

config system saml
  Description: Global settings for SAML authentication.
  set binding-protocol [post|redirect]
  set cert {string}
  set default-login-page [normal|sso]
  set default-profile {string}
  set entity-id {string}
  set idp-cert {string}
  set idp-entity-id {string}
  set idp-single-logout-url {string}
  set idp-single-sign-on-url {string}
  set life {integer}
  set portal-url {string}
  set role [identity-provider|service-provider]
  set server-address {string}
  config service-providers
    Description: Authorized service providers.
    edit <name>
      config assertion-attributes
        Description: Customized SAML attributes to send along with assertion.
        edit <name>
          set type [username|email|...]
        next
      end
      set idp-entity-id {string}
      set idp-single-logout-url {string}
    end
  end
end

```

```

        set idp-single-sign-on-url {string}
        set prefix {string}
        set sp-binding-protocol [post|redirect]
        set sp-cert {string}
        set sp-entity-id {string}
        set sp-portal-url {string}
        set sp-single-logout-url {string}
        set sp-single-sign-on-url {string}
    next
end
set single-logout-url {string}
set single-sign-on-url {string}
set status [enable|disable]
set tolerance {integer}
end

```

config system saml

Parameter	Description	Type	Size	Default						
binding-protocol	IdP Binding protocol.	option	-	redirect						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>post</i></td><td>HTTP POST binding.</td></tr><tr><td><i>redirect</i></td><td>HTTP Redirect binding.</td></tr></table>	Option	Description	<i>post</i>	HTTP POST binding.	<i>redirect</i>	HTTP Redirect binding.			
Option	Description									
<i>post</i>	HTTP POST binding.									
<i>redirect</i>	HTTP Redirect binding.									
cert	Certificate to sign SAML messages.	string	Maximum length: 35							
default-login-page	Choose default login page.	option	-	normal						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Use local login page as default.</td></tr><tr><td><i>sso</i></td><td>Use IdP's Single Sign-On page as default.</td></tr></table>	Option	Description	<i>normal</i>	Use local login page as default.	<i>sso</i>	Use IdP's Single Sign-On page as default.			
Option	Description									
<i>normal</i>	Use local login page as default.									
<i>sso</i>	Use IdP's Single Sign-On page as default.									
default-profile	Default profile for new SSO admin.	string	Maximum length: 35							
entity-id	SP entity ID.	string	Maximum length: 255							
idp-cert	IDP certificate name.	string	Maximum length: 35							
idp-entity-id	IDP entity ID.	string	Maximum length: 255							

Parameter	Description	Type	Size	Default
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
life	Length of the range of time when the assertion is valid (in minutes).	integer	Minimum value: 30 0 Maximum value: 4294967295	
portal-url	SP portal URL. Read-only.	string	Maximum length: 255	
role	SAML role.	option	-	service-provider
	Option	Description		
	identity-provider	Identity Provider.		
	service-provider	Service Provider.		
server-address	Server address.	string	Maximum length: 63	
single-logout-url	SP single logout URL. Read-only.	string	Maximum length: 255	
single-sign-on-url	SP single sign-on URL. Read-only.	string	Maximum length: 255	
status	Enable/disable SAML authentication (default = disable).	option	-	disable
	Option	Description		
	enable	Enable SAML authentication.		
	disable	Disable SAML authentication.		
tolerance	Tolerance to the range of time when the assertion is valid (in minutes).	integer	Minimum value: 5 0 Maximum value: 4294967295	

config service-providers

Parameter	Description	Type	Size	Default
idp-entity-id	IDP entity ID. Read-only.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout URL. Read-only.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL. Read-only.	string	Maximum length: 255	
name	Name.	string	Maximum length: 35	
prefix	Prefix.	string	Maximum length: 35	
sp-binding-protocol	SP binding protocol.	option	-	post
	Option	Description		
	post	HTTP POST binding.		
	redirect	HTTP Redirect binding.		
sp-cert	SP certificate name.	string	Maximum length: 35	
sp-entity-id	SP entity ID.	string	Maximum length: 255	
sp-portal-url	SP portal URL.	string	Maximum length: 255	
sp-single-logout-url	SP single logout URL.	string	Maximum length: 255	
sp-single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	

config assertion-attributes

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Type.	option	-	username

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>username</i>	User Name.		
	<i>email</i>	Email Address.		
	<i>profile-name</i>	Profile Name.		

config system sdn-connector

Configure connection to SDN Connector.

```

config system sdn-connector
  Description: Configure connection to SDN Connector.
  edit <name>
    set access-key {string}
    set alt-resource-ip [disable|enable]
    set api-key {password}
    set azure-region [global|china|...]
    set client-id {string}
    set client-secret {password}
    config compartment-list
      Description: Configure OCI compartment list.
      edit <compartment-id>
      next
    end
    set domain {string}
    config external-account-list
      Description: Configure AWS external account list.
      edit <role-arn>
        set external-id {string}
        set region-list <region1>, <region2>, ...
      next
    end
    config external-ip
      Description: Configure GCP external IP.
      edit <name>
      next
    end
    config forwarding-rule
      Description: Configure GCP forwarding rule.
      edit <rule-name>
        set target {string}
      next
    end
    config gcp-project-list
      Description: Configure GCP project list.
      edit <id>
        set gcp-zone-list <name1>, <name2>, ...

```

```

        next
    end
    set group-name {string}
    set ha-status [disable|enable]
    set ibm-region [dallas|washington-dc|...]
    set login-endpoint {string}
    set message-server-port {integer}
    set microsoft-365 [disable|enable]
    config nic
        Description: Configure Azure network interface.
        edit <name>
            config ip
                Description: Configure IP configuration.
                edit <name>
                    set private-ip {string}
                    set public-ip {string}
                    set resource-group {string}
                next
            end
            set peer-nic {string}
        next
    end
    set oci-cert {string}
    set oci-fingerprint {string}
    config oci-region-list
        Description: Configure OCI region list.
        edit <region>
            next
        end
    set oci-region-type [commercial|government]
    set password {password_aes256}
    set private-key {user}
    set proxy {string}
    set region {string}
    set resource-group {string}
    set resource-url {string}
    config route
        Description: Configure GCP route.
        edit <name>
            next
        end
    config route-table
        Description: Configure Azure route table.
        edit <name>
            set resource-group {string}
            config route
                Description: Configure Azure route.
                edit <name>
                    set next-hop {string}
                next
            end
            set subscription-id {string}

```

```

        next
    end
    set secret-key {password}
    set secret-token {user}
    set server {string}
    set server-ca-cert {string}
    set server-cert {string}
    set server-list <ip1>, <ip2>, ...
    set server-port {integer}
    set service-account {string}
    set status [disable|enable]
    set subscription-id {string}
    set tenant-id {string}
    set type [aci|alicloud|...]
    set update-interval {integer}
    set use-metadata-iam [disable|enable]
    set user-id {string}
    set username {string}
    set vcenter-password {password_aes256}
    set vcenter-server {string}
    set vcenter-username {string}
    set vdom {string}
    set verify-certificate [disable|enable]
    set vpc-id {string}
next
end

```

config system sdn-connector

Parameter	Description	Type	Size	Default
access-key	AWS / ACS access key ID.	string	Maximum length: 31	
alt-resource-ip	Enable/disable AWS alternative resource IP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable AWS alternative resource IP.		
	<i>enable</i>	Enable AWS alternative resource IP.		
api-key	IBM cloud API key or service ID API key.	password	Not Specified	
azure-region	Azure server region.	option	-	global
	Option	Description		
	<i>global</i>	Global Azure Server.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>china</i>	China Azure Server.		
	<i>germany</i>	Germany Azure Server.		
	<i>usgov</i>	US Government Azure Server.		
	<i>local</i>	Azure Stack Local Server.		
client-id	Azure client ID (application ID).	string	Maximum length: 63	
client-secret	Azure client secret (application key).	password	Not Specified	
domain	Domain name.	string	Maximum length: 127	
group-name	Full path group name of computers.	string	Maximum length: 127	
ha-status	Enable/disable use for FortiGate HA service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use for FortiGate HA service.		
	<i>enable</i>	Enable use for FortiGate HA service.		
ibm-region	IBM cloud region name.	option	-	dallas
	Option	Description		
	<i>dallas</i>	US South (Dallas) Public Endpoint.		
	<i>washington-dc</i>	US East (Washington DC) Public Endpoint.		
	<i>london</i>	United Kingdom (London) Public Endpoint.		
	<i>frankfurt</i>	Germany (Frankfurt) Public Endpoint.		
	<i>sydney</i>	Australia (Sydney) Public Endpoint.		
	<i>tokyo</i>	Japan (Tokyo) Public Endpoint.		
	<i>osaka</i>	Japan (Osaka) Public Endpoint.		
	<i>toronto</i>	Canada (Toronto) Public Endpoint.		
	<i>sao-paulo</i>	Brazil (Sao Paulo) Public Endpoint.		
	<i>madrid</i>	Spain (Madrid) Public Endpoint.		
login-endpoint	Azure Stack login endpoint.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default						
message-server-port	HTTP port number of the SAP message server.	integer	Minimum value: 0 Maximum value: 65535	0						
microsoft-365	Enable to use as Microsoft 365 connector.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Azure SDN connector</td></tr><tr><td>enable</td><td>Microsoft 365 SDN connector</td></tr></table>				Option	Description	disable	Azure SDN connector	enable	Microsoft 365 SDN connector
	Option	Description								
	disable	Azure SDN connector								
enable	Microsoft 365 SDN connector									
name	SDN connector name.	string	Maximum length: 35							
oci-cert	OCI certificate.	string	Maximum length: 63							
oci-fingerprint	OCI pubkey fingerprint. Read-only.	string	Maximum length: 63							
oci-region-type	OCI region type.	option	-	commercial						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>commercial</td><td>Commercial region.</td></tr><tr><td>government</td><td>Government region.</td></tr></table>				Option	Description	commercial	Commercial region.	government	Government region.
	Option	Description								
	commercial	Commercial region.								
government	Government region.									
password	Password of the remote SDN connector as login credentials.	password_aes256	Not Specified							
private-key	Private key of GCP service account.	user	Not Specified							
proxy	SDN proxy.	string	Maximum length: 35							
region	AWS / ACS region name.	string	Maximum length: 31							
resource-group	Azure resource group.	string	Maximum length: 63							
resource-url	Azure Stack resource URL.	string	Maximum length: 127							
secret-key	AWS / ACS secret access key.	password	Not Specified							
secret-token	Secret token of Kubernetes service account.	user	Not Specified							

Parameter	Description	Type	Size	Default														
server	Server address of the remote SDN connector.	string	Maximum length: 127															
server-ca-cert	Trust only those servers whose certificate is directly/indirectly signed by this certificate.	string	Maximum length: 127															
server-cert	Trust servers that contain this certificate only.	string	Maximum length: 127															
server-list <ip>	Server address list of the remote SDN connector. IPv4 address.	string	Maximum length: 15															
server-port	Port number of the remote SDN connector.	integer	Minimum value: 0 Maximum value: 65535	0														
service-account	GCP service account email.	string	Maximum length: 127															
status	Enable/disable connection to the remote SDN connector.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable connection to this SDN Connector.</td></tr><tr><td><i>enable</i></td><td>Enable connection to this SDN Connector.</td></tr></table>				Option	Description	<i>disable</i>	Disable connection to this SDN Connector.	<i>enable</i>	Enable connection to this SDN Connector.								
Option	Description																	
<i>disable</i>	Disable connection to this SDN Connector.																	
<i>enable</i>	Enable connection to this SDN Connector.																	
subscription-id	Azure subscription ID.	string	Maximum length: 63															
tenant-id	Tenant ID (directory ID).	string	Maximum length: 127															
type	Type of SDN connector.	option	-	aws														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aci</i></td><td>Application Centric Infrastructure (ACI).</td></tr><tr><td><i>alicloud</i></td><td>AliCloud Service (ACS).</td></tr><tr><td><i>aws</i></td><td>Amazon Web Services (AWS).</td></tr><tr><td><i>azure</i></td><td>Microsoft Azure.</td></tr><tr><td><i>gcp</i></td><td>Google Cloud Platform (GCP).</td></tr><tr><td><i>nsx</i></td><td>VMware NSX.</td></tr></table>				Option	Description	<i>aci</i>	Application Centric Infrastructure (ACI).	<i>alicloud</i>	AliCloud Service (ACS).	<i>aws</i>	Amazon Web Services (AWS).	<i>azure</i>	Microsoft Azure.	<i>gcp</i>	Google Cloud Platform (GCP).	<i>nsx</i>	VMware NSX.
Option	Description																	
<i>aci</i>	Application Centric Infrastructure (ACI).																	
<i>alicloud</i>	AliCloud Service (ACS).																	
<i>aws</i>	Amazon Web Services (AWS).																	
<i>azure</i>	Microsoft Azure.																	
<i>gcp</i>	Google Cloud Platform (GCP).																	
<i>nsx</i>	VMware NSX.																	

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>nuage</i></td><td>Nuage VSP.</td></tr><tr><td><i>oci</i></td><td>Oracle Cloud Infrastructure.</td></tr><tr><td><i>openstack</i></td><td>OpenStack.</td></tr><tr><td><i>kubernetes</i></td><td>Kubernetes.</td></tr><tr><td><i>vmware</i></td><td>VMware vSphere (vCenter & ESXi).</td></tr><tr><td><i>sepm</i></td><td>Symantec Endpoint Protection Manager.</td></tr><tr><td><i>aci-direct</i></td><td>Application Centric Infrastructure (ACI Direct Connection).</td></tr><tr><td><i>ibm</i></td><td>IBM Cloud Infrastructure.</td></tr><tr><td><i>nutanix</i></td><td>Nutanix Prism Central.</td></tr><tr><td><i>sap</i></td><td>SAP Control.</td></tr></table>	Option	Description	<i>nuage</i>	Nuage VSP.	<i>oci</i>	Oracle Cloud Infrastructure.	<i>openstack</i>	OpenStack.	<i>kubernetes</i>	Kubernetes.	<i>vmware</i>	VMware vSphere (vCenter & ESXi).	<i>sepm</i>	Symantec Endpoint Protection Manager.	<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).	<i>ibm</i>	IBM Cloud Infrastructure.	<i>nutanix</i>	Nutanix Prism Central.	<i>sap</i>	SAP Control.			
	Option	Description																								
	<i>nuage</i>	Nuage VSP.																								
	<i>oci</i>	Oracle Cloud Infrastructure.																								
	<i>openstack</i>	OpenStack.																								
	<i>kubernetes</i>	Kubernetes.																								
	<i>vmware</i>	VMware vSphere (vCenter & ESXi).																								
	<i>sepm</i>	Symantec Endpoint Protection Manager.																								
	<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).																								
	<i>ibm</i>	IBM Cloud Infrastructure.																								
<i>nutanix</i>	Nutanix Prism Central.																									
<i>sap</i>	SAP Control.																									
update-interval	Dynamic object update interval (30 - 3600 sec, default = 60, 0 = disabled).	integer	Minimum value: 0 Maximum value: 3600	60																						
use-metadata-iam	Enable/disable use of IAM role from metadata to call API.	option	-	disable **																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable using IAM role to call API.</td></tr><tr><td><i>enable</i></td><td>Enable using IAM role to call API.</td></tr></table>	Option	Description	<i>disable</i>	Disable using IAM role to call API.	<i>enable</i>	Enable using IAM role to call API.																			
	Option	Description																								
	<i>disable</i>	Disable using IAM role to call API.																								
<i>enable</i>	Enable using IAM role to call API.																									
user-id	User ID.	string	Maximum length: 127																							
username	Username of the remote SDN connector as login credentials.	string	Maximum length: 64																							
vcenter-password	vCenter server password for NSX quarantine.	password_aes256	Not Specified																							
vcenter-server	vCenter server address for NSX quarantine.	string	Maximum length: 127																							
vcenter-username	vCenter server username for NSX quarantine.	string	Maximum length: 64																							
vdom	Virtual domain name of the remote SDN connector.	string	Maximum length: 31																							

Parameter	Description	Type	Size	Default						
verify-certificate	Enable/disable server certificate verification.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable server certificate verification.</td></tr><tr><td>enable</td><td>Enable server certificate verification.</td></tr></table>				Option	Description	disable	Disable server certificate verification.	enable	Enable server certificate verification.
Option	Description									
disable	Disable server certificate verification.									
enable	Enable server certificate verification.									
vpc-id	AWS VPC ID.	string	Maximum length: 31							

** Values may differ between models.

config compartment-list

Parameter	Description	Type	Size	Default
compartment-id	OCI compartment ID.	string	Maximum length: 127	

config external-account-list

Parameter	Description	Type	Size	Default
external-id	AWS external ID.	string	Maximum length: 1399	
region-list <region>	AWS region name list. AWS region name.	string	Maximum length: 31	
role-arn	AWS role ARN to assume.	string	Maximum length: 2047	

config external-ip

Parameter	Description	Type	Size	Default
name	External IP name.	string	Maximum length: 63	

config forwarding-rule

Parameter	Description	Type	Size	Default
rule-name	Forwarding rule name.	string	Maximum length: 63	
target	Target instance name.	string	Maximum length: 63	

config gcp-project-list

Parameter	Description	Type	Size	Default
gcp-zone-list <name>	Configure GCP zone list. GCP zone name.	string	Maximum length: 127	
id	GCP project ID.	string	Maximum length: 127	

config nic

Parameter	Description	Type	Size	Default
name	Network interface name.	string	Maximum length: 63	
peer-nic	Peer network interface name.	string	Maximum length: 63	

config ip

Parameter	Description	Type	Size	Default
name	IP configuration name.	string	Maximum length: 63	
private-ip	Private IP address.	string	Maximum length: 39	
public-ip	Public IP name.	string	Maximum length: 63	
resource-group	Resource group of Azure public IP.	string	Maximum length: 63	

config oci-region-list

Parameter	Description	Type	Size	Default
region	OCI region.	string	Maximum length: 31	

config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	

config route-table

Parameter	Description	Type	Size	Default
name	Route table name.	string	Maximum length: 63	
resource-group	Resource group of Azure route table.	string	Maximum length: 63	
subscription-id	Subscription ID of Azure route table.	string	Maximum length: 63	

config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	
next-hop	Next hop address.	string	Maximum length: 127	

config system sdn-proxy

Configure SDN proxy.

```
config system sdn-proxy
  Description: Configure SDN proxy.
  edit <name>
    set password {password_aes256}
    set server {string}
    set server-port {integer}
    set type [general|fortimanager]
    set username {string}
```

```
next
end
```

config system sdn-proxy

Parameter	Description	Type	Size	Default						
name	SDN proxy name.	string	Maximum length: 35							
password	SDN proxy password.	password_aes256	Not Specified							
server	Server address of the SDN proxy.	string	Maximum length: 127							
server-port	Port number of the SDN proxy.	integer	Minimum value: 0 Maximum value: 65535	0						
type	Type of SDN proxy.	option	-	general						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>general</i></td><td>General HTTP proxy.</td></tr><tr><td><i>fortimanager</i></td><td>FortiManager SDN proxy.</td></tr></table>				Option	Description	<i>general</i>	General HTTP proxy.	<i>fortimanager</i>	FortiManager SDN proxy.
Option	Description									
<i>general</i>	General HTTP proxy.									
<i>fortimanager</i>	FortiManager SDN proxy.									
username	SDN proxy username.	string	Maximum length: 64							

config system sdn-vpn

Configure public cloud VPN service.

```
config system sdn-vpn
  Description: Configure public cloud VPN service.
  edit <name>
    set bgp-as {integer}
    set cgw-gateway {ipv4-address-any}
    set cgw-name {string}
    set code {integer}
    set internal-interface {string}
    set local-cidr {ipv4-classnet}
    set nat-traversal [disable|enable]
    set psksecret {password-3}
    set remote-cidr {ipv4-classnet}
    set remote-type [vgw|tgw]
```

```

    set routing-type [static|dynamic]
    set sdn {string}
    set status {integer}
    set subnet-id {string}
    set tgw-id {string}
    set tunnel-interface {string}
    set type {integer}
    set vgw-id {string}
  next
end

```

config system sdn-vpn

Parameter	Description	Type	Size	Default
bgp-as	BGP Router AS number.	integer	Minimum value: 1 Maximum value: 4294967295	65000
cgw-gateway	Public IP address of the customer gateway.	ipv4-address-any	Not Specified	0.0.0.0
cgw-name	AWS customer gateway name to be created.	string	Maximum length: 35	
code	SDN VPN error code. Read-only.	integer	Minimum value: 0 Maximum value: 255	0
internal-interface	Internal interface with local subnet.	string	Maximum length: 15	
local-cidr	Local subnet address and subnet mask.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
name	Public cloud VPN name.	string	Maximum length: 35	
nat-traversal	Enable/disable use for NAT traversal. Please enable if your FortiGate device is behind a NAT/PAT device.	option	-	enable
	Option	Description		
	disable	Disable NAT traversal.		
	enable	Enable NAT traversal.		
psksecret	Pre-shared secret for PSK authentication. Auto-generated if not specified	password-3	Not Specified	

Parameter	Description	Type	Size	Default
remote-cidr	Remote subnet address and subnet mask.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
remote-type	Type of remote device.	option	-	vgw
	Option	Description		
	vgw	Virtual private gateway.		
	tgw	Transit gateway.		
routing-type	Type of routing.	option	-	dynamic
	Option	Description		
	static	Static routing.		
	dynamic	Dynamic routing.		
sdn	SDN connector name.	string	Maximum length: 35	
status	SDN VPN status. Read-only.	integer	Minimum value: 0 Maximum value: 255	
subnet-id	AWS subnet id for TGW route propagation.	string	Maximum length: 63	
tgw-id	Transit gateway id.	string	Maximum length: 63	
tunnel-interface	Tunnel interface with public IP.	string	Maximum length: 15	
type	SDN VPN type. Read-only.	integer	Minimum value: 0 Maximum value: 65535	
vgw-id	Virtual private gateway id.	string	Maximum length: 63	

config system sdwan

Configure redundant Internet connections with multiple outbound links and health-check profiles.

```
config system sdwan
  Description: Configure redundant Internet connections with multiple outbound links and health-check profiles.
  set app-perf-log-period {integer}
  config duplication
    Description: Create SD-WAN duplication rule.
```

```

edit <id>
    set dstaddr <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set packet-de-duplication [enable|disable]
    set packet-duplication [disable|force|...]
    set service <name1>, <name2>, ...
    set service-id <id1>, <id2>, ...
    set sla-match-service [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set srcintf <name1>, <name2>, ...
next
end
set duplication-max-discrepancy {integer}
set duplication-max-num {integer}
set fail-alert-interfaces <name1>, <name2>, ...
set fail-detect [enable|disable]
config health-check

```

Description: SD-WAN status checking or health checking. Identify a server on the Internet and determine how SD-WAN verifies that the FortiGate can communicate with it.

```

edit <name>
    set addr-mode [ipv4|ipv6]
    set agent-probe-timeout {integer}
    set class-id {integer}
    set detect-mode [active|passive|...]
    set diffservcode {user}
    set dns-match-ip {ipv4-address}
    set dns-request-domain {string}
    set embed-measured-health [enable|disable]
    set failtime {integer}
    set fortiguard [disable|enable]
    set fortiguard-name {string}
    set ftp-file {string}
    set ftp-mode [passive|port]
    set ha-priority {integer}
    set http-agent {string}
    set http-get {string}
    set http-match {string}
    set interval {integer}
    set members <seq-num1>, <seq-num2>, ...
    set mos-codec [g711|g722|...]
    set packet-size {integer}
    set password {password}
    set port {integer}
    set probe-count {integer}
    set probe-packets [disable|enable]
    set probe-timeout {integer}
    set protocol [ping|tcp-echo|...]
    set quality-measured-method [half-open|half-close]
    set recoverytime {integer}
    set remote-probe-timeout {integer}

```

```

set security-mode [none|authentication]
set server {string}
config sla
    Description: Service level agreement (SLA).
    edit <id>
        set jitter-threshold {integer}
        set latency-threshold {integer}
        set link-cost-factor {option1}, {option2}, ...
        set mos-threshold {string}
        set packetloss-threshold {integer}
        set priority-in-sla {integer}
        set priority-out-sla {integer}
    next
end
set sla-fail-log-period {integer}
set sla-id-redistribute {integer}
set sla-pass-log-period {integer}
set source {ipv4-address}
set source6 {ipv6-address}
set system-dns [disable|enable]
set threshold-alert-jitter {integer}
set threshold-alert-latency {integer}
set threshold-alert-packetloss {integer}
set threshold-warning-jitter {integer}
set threshold-warning-latency {integer}
set threshold-warning-packetloss {integer}
set update-cascade-interface [enable|disable]
set update-static-route [enable|disable]
set user {string}
set vrf {integer}
next
end
set load-balance-mode [source-ip-based|weight-based|...]
config members
    Description: FortiGate interfaces added to the SD-WAN.
    edit <seq-num>
        set comment {var-string}
        set cost {integer}
        set gateway {ipv4-address}
        set gateway6 {ipv6-address}
        set ingress-spillover-threshold {integer}
        set interface {string}
        set preferred-source {ipv4-address}
        set priority {integer}
        set priority-in-sla {integer}
        set priority-out-sla {integer}
        set priority6 {integer}
        set source {ipv4-address}
        set source6 {ipv6-address}
        set spillover-threshold {integer}
        set status [disable|enable]
        set transport-group {integer}
    
```

```

        set volume-ratio {integer}
        set weight {integer}
        set zone {string}
    next
end
config neighbor
    Description: Create SD-WAN neighbor from BGP neighbor table to control route
    advertisements according to SLA status.
    edit <ip>
        set health-check {string}
        set member <seq-num1>, <seq-num2>, ...
        set minimum-sla-meet-members {integer}
        set mode [sla|speedtest]
        set role [standalone|primary|...]
        set route-metric [preferable|priority]
        set service-id {integer}
        set sla-id {integer}
    next
end
set neighbor-hold-boot-time {integer}
set neighbor-hold-down [enable|disable]
set neighbor-hold-down-time {integer}
config service
    Description: Create SD-WAN rules (also called services) to control how sessions are
    distributed to interfaces in the SD-WAN.
    edit <id>
        set addr-mode [ipv4|ipv6]
        set agent-exclusive [enable|disable]
        set bandwidth-weight {integer}
        set comment {var-string}
        set default [enable|disable]
        set dscp-forward [enable|disable]
        set dscp-forward-tag {user}
        set dscp-reverse [enable|disable]
        set dscp-reverse-tag {user}
        set dst <name1>, <name2>, ...
        set dst-negate [enable|disable]
        set dst6 <name1>, <name2>, ...
        set end-port {integer}
        set end-src-port {integer}
        set fib-best-match-force [disable|enable]
        set gateway [enable|disable]
        set groups <name1>, <name2>, ...
        set hash-mode [round-robin|source-ip-based|...]
        set health-check <name1>, <name2>, ...
        set hold-down-time {integer}
        set input-device <name1>, <name2>, ...
        set input-device-negate [enable|disable]
        set input-zone <name1>, <name2>, ...
        set internet-service [enable|disable]
        set internet-service-app-ctrl <id1>, <id2>, ...
        set internet-service-app-ctrl-category <id1>, <id2>, ...

```



```

set internet-service-app-ctrl-group <name1>, <name2>, ...
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-name <name1>, <name2>, ...
set jitter-weight {integer}
set latency-weight {integer}
set link-cost-factor [latency|jitter|...]
set link-cost-threshold {integer}
set load-balance [enable|disable]
set minimum-sla-meet-members {integer}
set mode [auto|manual|...]
set name {string}
set packet-loss-weight {integer}
set passive-measurement [enable|disable]
set priority-members <seq-num1>, <seq-num2>, ...
set priority-zone <name1>, <name2>, ...
set protocol {integer}
set quality-link {integer}
set role [standalone|primary|...]
set shortcut [enable|disable]
set shortcut-priority [enable|disable|...]
config sla
    Description: Service level agreement (SLA).
    edit <health-check>
        set id {integer}
    next
end
set sla-compare-method [order|number]
set sla-stickiness [enable|disable]
set src <name1>, <name2>, ...
set src-negate [enable|disable]
set src6 <name1>, <name2>, ...
set standalone-action [enable|disable]
set start-port {integer}
set start-src-port {integer}
set status [enable|disable]
set tie-break [zone|cfg-order|...]
set tos {user}
set tos-mask {user}
set use-shortcut-sla [enable|disable]
set users <name1>, <name2>, ...
set zone-mode [enable|disable]
next
end
set speedtest-bypass-routing [disable|enable]
set status [disable|enable]
config zone
    Description: Configure SD-WAN zones.
    edit <name>
        set advpn-health-check {string}
        set advpn-select [enable|disable]

```

```

        set minimum-sla-meet-members {integer}
        set service-sla-tie-break [cfg-order|fib-best-match|...]
    next
end
end

```

config system sdwan

Parameter	Description	Type	Size	Default						
app-perf-log-period	Time interval in seconds that application performance logs are generated (0 - 3600, default = 0).	integer	Minimum value: 0 Maximum value: 3600	0						
duplication-max-discrepancy	Maximum discrepancy between two packets for deduplication in milliseconds (250 - 1000, default = 250).	integer	Minimum value: 250 Maximum value: 1000	250						
duplication-max-num	Maximum number of interface members a packet is duplicated in the SD-WAN zone (2 - 4, default = 2; if set to 3, the original packet plus 2 more copies are created).	integer	Minimum value: 2 Maximum value: 4	2						
fail-alert-interfaces <name>	Physical interfaces that will be alerted. Physical interface name.	string	Maximum length: 79							
fail-detect	Enable/disable SD-WAN Internet connection status checking (failure detection).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable status checking.</td></tr><tr><td>disable</td><td>Disable status checking.</td></tr></table>	Option	Description	enable	Enable status checking.	disable	Disable status checking.			
Option	Description									
enable	Enable status checking.									
disable	Disable status checking.									
load-balance-mode	Algorithm or mode to use for load balancing Internet traffic to SD-WAN members.	option	-	source-ip-based						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>source-ip-based</td><td>Source IP load balancing. All traffic from a source IP is sent to the same interface.</td></tr><tr><td>weight-based</td><td>Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.</td></tr></table>	Option	Description	source-ip-based	Source IP load balancing. All traffic from a source IP is sent to the same interface.	weight-based	Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.			
Option	Description									
source-ip-based	Source IP load balancing. All traffic from a source IP is sent to the same interface.									
weight-based	Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.									

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>usage-based</td><td>Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.</td></tr><tr><td>source-dest-ip-based</td><td>Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.</td></tr><tr><td>measured-volume-based</td><td>Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.</td></tr></table>	Option	Description	usage-based	Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.	source-dest-ip-based	Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.	measured-volume-based	Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.			
	Option	Description										
	usage-based	Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.										
	source-dest-ip-based	Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.										
measured-volume-based	Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.											
neighbor-hold-boot-time	Waiting period in seconds when switching from the primary neighbor to the secondary neighbor from the neighbor start. (0 - 10000000, default = 0).	integer	Minimum value: 0 Maximum value: 10000000	0								
neighbor-hold-down	Enable/disable hold switching from the secondary neighbor to the primary neighbor.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable hold switching from the secondary neighbor to the primary neighbor.</td></tr><tr><td>disable</td><td>Disable hold switching from the secondary neighbor to the primary neighbor.</td></tr></table>	Option	Description	enable	Enable hold switching from the secondary neighbor to the primary neighbor.	disable	Disable hold switching from the secondary neighbor to the primary neighbor.					
	Option	Description										
	enable	Enable hold switching from the secondary neighbor to the primary neighbor.										
disable	Disable hold switching from the secondary neighbor to the primary neighbor.											
neighbor-hold-down-time	Waiting period in seconds when switching from the secondary neighbor to the primary neighbor when hold-down is disabled. (0 - 10000000, default = 0).	integer	Minimum value: 0 Maximum value: 10000000	0								
speedtest-bypass-routing	Enable/disable bypass routing when speedtest on a SD-WAN member.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SD-WAN.</td></tr><tr><td>enable</td><td>Enable SD-WAN.</td></tr></table>	Option	Description	disable	Disable SD-WAN.	enable	Enable SD-WAN.					
	Option	Description										
	disable	Disable SD-WAN.										
enable	Enable SD-WAN.											
status	Enable/disable SD-WAN.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SD-WAN.</td></tr><tr><td>enable</td><td>Enable SD-WAN.</td></tr></table>	Option	Description	disable	Disable SD-WAN.	enable	Enable SD-WAN.					
	Option	Description										
	disable	Disable SD-WAN.										
enable	Enable SD-WAN.											

config duplication

Parameter	Description	Type	Size	Default								
dstaddr <name>	Destination address or address group names. Address or address group name.	string	Maximum length: 79									
dstaddr6 <name>	Destination address6 or address6 group names. Address6 or address6 group name.	string	Maximum length: 79									
dstintf <name>	Outgoing (egress) interfaces or zones. Interface, zone or SDWAN zone name.	string	Maximum length: 79									
id	Duplication rule ID (1 - 255).	integer	Minimum value: 0 1 Maximum value: 255									
packet-de- duplication	Enable/disable discarding of packets that have been duplicated.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable discarding of packets that have been duplicated.</td></tr><tr><td>disable</td><td>Disable discarding of packets that have been duplicated.</td></tr></table>				Option	Description	enable	Enable discarding of packets that have been duplicated.	disable	Disable discarding of packets that have been duplicated.		
Option	Description											
enable	Enable discarding of packets that have been duplicated.											
disable	Disable discarding of packets that have been duplicated.											
packet- duplication	Configure packet duplication method.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable packet duplication.</td></tr><tr><td>force</td><td>Duplicate packets across all interface members of the SD-WAN zone.</td></tr><tr><td>on-demand</td><td>Duplicate packets across all interface members of the SD-WAN zone based on the link quality.</td></tr></table>				Option	Description	disable	Disable packet duplication.	force	Duplicate packets across all interface members of the SD-WAN zone.	on-demand	Duplicate packets across all interface members of the SD-WAN zone based on the link quality.
Option	Description											
disable	Disable packet duplication.											
force	Duplicate packets across all interface members of the SD-WAN zone.											
on-demand	Duplicate packets across all interface members of the SD-WAN zone based on the link quality.											
service <name>	Service and service group name. Service and service group name.	string	Maximum length: 79									
service-id <id>	SD-WAN service rule ID list. SD-WAN service rule ID.	integer	Minimum value: 0 Maximum value: 4294967295									
sla-match- service	Enable/disable packet duplication matching health-check SLAs in service rule.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable packet duplication matching health-check SLAs in service rule (matching all SLAs of current defined service).</td></tr></table>				Option	Description	enable	Enable packet duplication matching health-check SLAs in service rule (matching all SLAs of current defined service).				
Option	Description											
enable	Enable packet duplication matching health-check SLAs in service rule (matching all SLAs of current defined service).											

Parameter	Description	Type	Size	Default				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet duplication matching health-check SLAs in service rule (matching all SLAs of all defined health-check).</td></tr></table>	Option	Description	<i>disable</i>	Disable packet duplication matching health-check SLAs in service rule (matching all SLAs of all defined health-check).			
Option	Description							
<i>disable</i>	Disable packet duplication matching health-check SLAs in service rule (matching all SLAs of all defined health-check).							
srcaddr <name>	Source address or address group names. Address or address group name.	string	Maximum length: 79					
srcaddr6 <name>	Source address6 or address6 group names. Address6 or address6 group name.	string	Maximum length: 79					
srcintf <name>	Incoming (ingress) interfaces or zones. Interface, zone or SDWAN zone name.	string	Maximum length: 79					

config health-check

Parameter	Description	Type	Size	Default												
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 mode.</td></tr><tr><td>ipv6</td><td>IPv6 mode.</td></tr></table>				Option	Description	ipv4	IPv4 mode.	ipv6	IPv6 mode.						
Option	Description															
ipv4	IPv4 mode.															
ipv6	IPv6 mode.															
agent-probe-timeout	Time to wait before a probe packet is considered lost when detect-mode is agent (5000 - 3600*1000 msec, default = 60000).	integer	Minimum value: 5000 Maximum value: 3600000	60000												
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
detect-mode	The mode determining how to detect the server.	option	-	active												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>active</td><td>The probes are sent actively.</td></tr><tr><td>passive</td><td>The traffic measures health without probes.</td></tr><tr><td>prefer-passive</td><td>The probes are sent in case of no new traffic.</td></tr><tr><td>remote</td><td>Link health obtained from remote peers.</td></tr><tr><td>agent-based</td><td>Traffic health is measured from the fabric connectors.</td></tr></table>				Option	Description	active	The probes are sent actively.	passive	The traffic measures health without probes.	prefer-passive	The probes are sent in case of no new traffic.	remote	Link health obtained from remote peers.	agent-based	Traffic health is measured from the fabric connectors.
Option	Description															
active	The probes are sent actively.															
passive	The traffic measures health without probes.															
prefer-passive	The probes are sent in case of no new traffic.															
remote	Link health obtained from remote peers.															
agent-based	Traffic health is measured from the fabric connectors.															

Parameter	Description	Type	Size	Default						
diffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified							
dns-match-ip	Response IP expected from DNS server if the protocol is DNS.	ipv4-address	Not Specified	0.0.0.0						
dns-request-domain	Fully qualified domain name to resolve for the DNS probe.	string	Maximum length: 255	www.example.com						
embed-measured-health	Enable/disable embedding measured health information.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable embed measured health.</td></tr><tr><td><i>disable</i></td><td>Disable embed measured health.</td></tr></table>				Option	Description	<i>enable</i>	Enable embed measured health.	<i>disable</i>	Disable embed measured health.
Option	Description									
<i>enable</i>	Enable embed measured health.									
<i>disable</i>	Disable embed measured health.									
failtime	Number of failures before server is considered lost (1 - 3600, default = 5).	integer	Minimum value: 1 Maximum value: 3600	5						
fortiguard	Enable/disable use of FortiGuard predefined server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of FortiGuard predefined server.</td></tr><tr><td><i>enable</i></td><td>Enable use of FortiGuard predefined server.</td></tr></table>				Option	Description	<i>disable</i>	Disable use of FortiGuard predefined server.	<i>enable</i>	Enable use of FortiGuard predefined server.
Option	Description									
<i>disable</i>	Disable use of FortiGuard predefined server.									
<i>enable</i>	Enable use of FortiGuard predefined server.									
fortiguard-name	Predefined health-check target name.	string	Maximum length: 35							
ftp-file	Full path and file name on the FTP server to download for FTP health-check to probe.	string	Maximum length: 254							
ftp-mode	FTP mode.	option	-	passive						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>passive</i></td><td>The FTP health-check initiates and establishes the data connection.</td></tr><tr><td><i>port</i></td><td>The FTP server initiates and establishes the data connection.</td></tr></table>				Option	Description	<i>passive</i>	The FTP health-check initiates and establishes the data connection.	<i>port</i>	The FTP server initiates and establishes the data connection.
Option	Description									
<i>passive</i>	The FTP health-check initiates and establishes the data connection.									
<i>port</i>	The FTP server initiates and establishes the data connection.									
ha-priority	HA election priority (1 - 50).	integer	Minimum value: 1 Maximum value: 50							

Parameter	Description	Type	Size	Default								
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/								
http-get	URL used to communicate with the server if the protocol if the protocol is HTTP.	string	Maximum length: 1024	/								
http-match	Response string expected from the server if the protocol is HTTP.	string	Maximum length: 1024									
interval	Status check interval in milliseconds, or the time between attempting to connect to the server (20 - 3600*1000 msec, default = 500).	integer	Minimum value: 20 Maximum value: 3600000	500								
members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295									
mos-codec	Codec to use for MOS calculation (default = g711).	option	-	g711								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>g711</td><td>Calculate MOS based on the G.711 codec.</td></tr><tr><td>g722</td><td>Calculate MOS based on the G.722 codec.</td></tr><tr><td>g729</td><td>Calculate MOS based on the G.729 codec.</td></tr></table>				Option	Description	g711	Calculate MOS based on the G.711 codec.	g722	Calculate MOS based on the G.722 codec.	g729	Calculate MOS based on the G.729 codec.
Option	Description											
g711	Calculate MOS based on the G.711 codec.											
g722	Calculate MOS based on the G.722 codec.											
g729	Calculate MOS based on the G.729 codec.											
name	Status check or health check name.	string	Maximum length: 35									
packet-size	Packet size of a TWAMP test session. (124/158 - 1024)	integer	Minimum value: 124 0 Maximum value: 65535									
password	TWAMP controller password in authentication mode.	password	Not Specified									
port	Port number used to communicate with the server over the selected protocol (0 - 65535, default = 0, auto select. http, tcp-connect: 80, udp-echo, tcp-echo: 7, dns: 53, ftp: 21, twamp: 862).	integer	Minimum value: 0 0 Maximum value: 65535									

Parameter	Description	Type	Size	Default																				
probe-count	Number of most recent probes that should be used to calculate latency and jitter (5 - 30, default = 30).	integer	Minimum value: 5 Maximum value: 30	30																				
probe-packets	Enable/disable transmission of probe packets.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable transmission of probe packets.</td></tr><tr><td>enable</td><td>Enable transmission of probe packets.</td></tr></table>	Option	Description	disable	Disable transmission of probe packets.	enable	Enable transmission of probe packets.																	
Option	Description																							
disable	Disable transmission of probe packets.																							
enable	Enable transmission of probe packets.																							
probe-timeout	Time to wait before a probe packet is considered lost (20 - 3600*1000 msec, default = 500).	integer	Minimum value: 20 Maximum value: 3600000	500																				
protocol	Protocol used to determine if the FortiGate can communicate with the server.	option	-	ping																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>Use PING to test the link with the server.</td></tr><tr><td>tcp-echo</td><td>Use TCP echo to test the link with the server.</td></tr><tr><td>udp-echo</td><td>Use UDP echo to test the link with the server.</td></tr><tr><td>http</td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td>https</td><td>Use HTTPS-GET to test the link with the server.</td></tr><tr><td>twamp</td><td>Use TWAMP to test the link with the server.</td></tr><tr><td>dns</td><td>Use DNS query to test the link with the server.</td></tr><tr><td>tcp-connect</td><td>Use a full TCP connection to test the link with the server.</td></tr><tr><td>ftp</td><td>Use FTP to test the link with the server.</td></tr></table>	Option	Description	ping	Use PING to test the link with the server.	tcp-echo	Use TCP echo to test the link with the server.	udp-echo	Use UDP echo to test the link with the server.	http	Use HTTP-GET to test the link with the server.	https	Use HTTPS-GET to test the link with the server.	twamp	Use TWAMP to test the link with the server.	dns	Use DNS query to test the link with the server.	tcp-connect	Use a full TCP connection to test the link with the server.	ftp	Use FTP to test the link with the server.			
Option	Description																							
ping	Use PING to test the link with the server.																							
tcp-echo	Use TCP echo to test the link with the server.																							
udp-echo	Use UDP echo to test the link with the server.																							
http	Use HTTP-GET to test the link with the server.																							
https	Use HTTPS-GET to test the link with the server.																							
twamp	Use TWAMP to test the link with the server.																							
dns	Use DNS query to test the link with the server.																							
tcp-connect	Use a full TCP connection to test the link with the server.																							
ftp	Use FTP to test the link with the server.																							
quality-measured-method	Method to measure the quality of tcp-connect.	option	-	half-open																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>half-open</td><td>Measure the round trip between syn and ack.</td></tr><tr><td>half-close</td><td>Measure the round trip between fin and ack.</td></tr></table>	Option	Description	half-open	Measure the round trip between syn and ack.	half-close	Measure the round trip between fin and ack.																	
Option	Description																							
half-open	Measure the round trip between syn and ack.																							
half-close	Measure the round trip between fin and ack.																							

Parameter	Description	Type	Size	Default						
recoverytime	Number of successful responses received before server is considered recovered (1 - 3600, default = 5).	integer	Minimum value: 1 Maximum value: 3600	5						
remote-probe-timeout	Time to wait before a probe packet is considered lost when detect-mode is remote (20 - 3600*1000 msec, default = 5000).	integer	Minimum value: 20 Maximum value: 3600000	5000						
security-mode	Twamp controller security mode.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Unauthenticated mode.</td></tr><tr><td>authentication</td><td>Authenticated mode.</td></tr></table>				Option	Description	none	Unauthenticated mode.	authentication	Authenticated mode.
Option	Description									
none	Unauthenticated mode.									
authentication	Authenticated mode.									
server	IP address or FQDN name of the server.	string	Maximum length: 79							
sla-fail-log-period	Time interval in seconds that SLA fail log messages will be generated (0 - 3600, default = 0).	integer	Minimum value: 0 Maximum value: 3600	0						
sla-id-redistribute	Select the ID from the SLA sub-table. The selected SLA's priority value will be distributed into the routing table (0 - 32, default = 0).	integer	Minimum value: 0 Maximum value: 32	0						
sla-pass-log-period	Time interval in seconds that SLA pass log messages will be generated (0 - 3600, default = 0).	integer	Minimum value: 0 Maximum value: 3600	0						
source	Source IP address used in the health-check packet to the server.	ipv4-address	Not Specified	0.0.0.0						
source6	Source IPv6 address used in the health-check packet to server.	ipv6-address	Not Specified	::						
system-dns	Enable/disable system DNS as the probe server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable system DNS as the probe server.</td></tr><tr><td>enable</td><td>Enable system DNS as the probe server.</td></tr></table>				Option	Description	disable	Disable system DNS as the probe server.	enable	Enable system DNS as the probe server.
Option	Description									
disable	Disable system DNS as the probe server.									
enable	Enable system DNS as the probe server.									

Parameter	Description	Type	Size	Default
threshold-alert-jitter	Alert threshold for jitter (ms, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-alert-latency	Alert threshold for latency (ms, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-alert-packetloss	Alert threshold for packet loss (percentage, default = 0).	integer	Minimum value: 0 Maximum value: 100	0
threshold-warning-jitter	Warning threshold for jitter (ms, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-warning-latency	Warning threshold for latency (ms, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-warning-packetloss	Warning threshold for packet loss (percentage, default = 0).	integer	Minimum value: 0 Maximum value: 100	0
update-cascade-interface	Enable/disable update cascade interface.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable update cascade interface.	
	<i>disable</i>		Disable update cascade interface.	
update-static-route	Enable/disable updating the static route.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable updating the static route.	
	<i>disable</i>		Disable updating the static route.	
user	The user name to access probe server.	string	Maximum length: 64	
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 511	0

config sla

Parameter	Description	Type	Size	Default
id	SLA ID.	integer	Minimum value: 1 Maximum value: 32	0
jitter-threshold	Jitter for SLA to make decision in milliseconds. (0 - 10000000, default = 5).	integer	Minimum value: 0 Maximum value: 10000000	5
latency-threshold	Latency for SLA to make decision in milliseconds. (0 - 10000000, default = 5).	integer	Minimum value: 0 Maximum value: 10000000	5
link-cost-factor	Criteria on which to base link selection.	option	-	latency jitter packet-loss
	Option	Description		
	latency	Select link based on latency.		
	jitter	Select link based on jitter.		
	packet-loss	Select link based on packet loss.		
	mos	Select link based on Mean Opinion Score (MOS).		
	remote	Select link based on available remote SLA status.		
mos-threshold	Minimum Mean Opinion Score for SLA to be marked as pass. (1.0 - 5.0, default = 3.6).	string	Maximum length: 35	3.6
packetloss-threshold	Packet loss for SLA to make decision in percentage. (0 - 100, default = 0).	integer	Minimum value: 0 Maximum value: 100	0
priority-in-sla	Value to be distributed into routing table when in-sla (0 - 65535, default = 0).	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
priority-out-sla	Value to be distributed into routing table when out-sla (0 - 65535, default = 0).	integer	Minimum value: 0 Maximum value: 65535	0

config members

Parameter	Description	Type	Size	Default
comment	Comments.	var-string	Maximum length: 255	
cost	Cost of this interface for services in SLA mode (0 - 4294967295, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
gateway	The default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.	ipv4-address	Not Specified	0.0.0.0
gateway6	IPv6 gateway.	ipv6-address	Not Specified	::
ingress-spillover-threshold	Ingress spillover threshold for this interface (0 - 16776000 kbit/s). When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000	0
interface	Interface name.	string	Maximum length: 15	
preferred-source	Preferred source of route for this member.	ipv4-address	Not Specified	0.0.0.0
priority	Priority of the interface for IPv4 (1 - 65535, default = 1). Used for SD-WAN rules or priority rules.	integer	Minimum value: 1 Maximum value: 65535	1
priority-in-sla	Preferred priority of routes to this member when this member is in-sla (0 - 65535, default = 0).	integer	Minimum value: 0 Maximum value: 65535	0
priority-out-sla	Preferred priority of routes to this member when this member is out-of-sla (0 - 65535, default = 0).	integer	Minimum value: 0 Maximum value: 65535	0
priority6	Priority of the interface for IPv6 (1 - 65535, default = 1024). Used for SD-WAN rules or priority rules.	integer	Minimum value: 1 Maximum value: 65535	1024

Parameter	Description	Type	Size	Default						
seq-num	Sequence number(1-512).	integer	Minimum value: 0 Maximum value: 512	0						
source	Source IP address used in the health-check packet to the server.	ipv4-address	Not Specified	0.0.0.0						
source6	Source IPv6 address used in the health-check packet to the server.	ipv6-address	Not Specified	::						
spillover-threshold	Egress spillover threshold for this interface (0 - 16776000 kbit/s). When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000	0						
status	Enable/disable this interface in the SD-WAN.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this interface in the SD-WAN.</td></tr><tr><td><i>enable</i></td><td>Enable this interface in the SD-WAN.</td></tr></table>				Option	Description	<i>disable</i>	Disable this interface in the SD-WAN.	<i>enable</i>	Enable this interface in the SD-WAN.
Option	Description									
<i>disable</i>	Disable this interface in the SD-WAN.									
<i>enable</i>	Enable this interface in the SD-WAN.									
transport-group	Measured transport group (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0						
volume-ratio	Measured volume ratio (this value / sum of all values = percentage of link volume, 1 - 255).	integer	Minimum value: 1 Maximum value: 255	1						
weight	Weight of this interface for weighted load balancing. (1 - 255) More traffic is directed to interfaces with higher weights.	integer	Minimum value: 1 Maximum value: 255	1						
zone	Zone name.	string	Maximum length: 35	virtual-wan-link						

config neighbor

Parameter	Description	Type	Size	Default
health-check	SD-WAN health-check name.	string	Maximum length: 35	
ip	IP/IPv6 address of neighbor or neighbor-group name.	string	Maximum length: 45	
member <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default								
minimum-sla-meet-members	Minimum number of members which meet SLA when the neighbor is preferred.	integer	Minimum value: 1 Maximum value: 255	1								
mode	What metric to select the neighbor.	option	-	sla								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sla</td><td>Select neighbor based on SLA link quality.</td></tr><tr><td>speedtest</td><td>Select neighbor based on the speedtest status.</td></tr></table>	Option	Description	sla	Select neighbor based on SLA link quality.	speedtest	Select neighbor based on the speedtest status.					
Option	Description											
sla	Select neighbor based on SLA link quality.											
speedtest	Select neighbor based on the speedtest status.											
role	Role of neighbor.	option	-	standalone								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>standalone</td><td>Standalone neighbor.</td></tr><tr><td>primary</td><td>Primary neighbor.</td></tr><tr><td>secondary</td><td>Secondary neighbor.</td></tr></table>	Option	Description	standalone	Standalone neighbor.	primary	Primary neighbor.	secondary	Secondary neighbor.			
Option	Description											
standalone	Standalone neighbor.											
primary	Primary neighbor.											
secondary	Secondary neighbor.											
route-metric	Route-metric of neighbor.	option	-	preferable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>preferable</td><td>Select neighbor based on its hc to match bgp preferable/unpreferable route_map.</td></tr><tr><td>priority</td><td>Select neighbor based on its members' priority-in-sla/priority-out-sla value.</td></tr></table>	Option	Description	preferable	Select neighbor based on its hc to match bgp preferable/unpreferable route_map.	priority	Select neighbor based on its members' priority-in-sla/priority-out-sla value.					
Option	Description											
preferable	Select neighbor based on its hc to match bgp preferable/unpreferable route_map.											
priority	Select neighbor based on its members' priority-in-sla/priority-out-sla value.											
service-id	SD-WAN service ID to work with the neighbor.	integer	Minimum value: 0 Maximum value: 4294967295	0								
sla-id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								

config service

Parameter	Description	Type	Size	Default						
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 mode.</td></tr><tr><td>ipv6</td><td>IPv6 mode.</td></tr></table>				Option	Description	ipv4	IPv4 mode.	ipv6	IPv6 mode.
	Option	Description								
	ipv4	IPv4 mode.								
ipv6	IPv6 mode.									

Parameter	Description	Type	Size	Default						
agent-exclusive	Set/unset the service as agent use exclusively.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Set the service as agent use exclusively.</td></tr><tr><td>disable</td><td>Unset the service as agent use exclusively.</td></tr></table>	Option	Description	enable	Set the service as agent use exclusively.	disable	Unset the service as agent use exclusively.			
	Option	Description								
	enable	Set the service as agent use exclusively.								
disable	Unset the service as agent use exclusively.									
bandwidth-weight	Coefficient of reciprocal of available bidirectional bandwidth in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000							
comment	Comments.	var-string	Maximum length: 255							
default	Enable/disable use of SD-WAN as default service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of SD-WAN as default service.</td></tr><tr><td>disable</td><td>Disable use of SD-WAN as default service.</td></tr></table>	Option	Description	enable	Enable use of SD-WAN as default service.	disable	Disable use of SD-WAN as default service.			
	Option	Description								
	enable	Enable use of SD-WAN as default service.								
disable	Disable use of SD-WAN as default service.									
dscp-forward	Enable/disable forward traffic DSCP tag.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of forward DSCP tag.</td></tr><tr><td>disable</td><td>Disable use of forward DSCP tag.</td></tr></table>	Option	Description	enable	Enable use of forward DSCP tag.	disable	Disable use of forward DSCP tag.			
	Option	Description								
	enable	Enable use of forward DSCP tag.								
disable	Disable use of forward DSCP tag.									
dscp-forward-tag	Forward traffic DSCP tag.	user	Not Specified							
dscp-reverse	Enable/disable reverse traffic DSCP tag.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of reverse DSCP tag.</td></tr><tr><td>disable</td><td>Disable use of reverse DSCP tag.</td></tr></table>	Option	Description	enable	Enable use of reverse DSCP tag.	disable	Disable use of reverse DSCP tag.			
	Option	Description								
	enable	Enable use of reverse DSCP tag.								
disable	Disable use of reverse DSCP tag.									
dscp-reverse-tag	Reverse traffic DSCP tag.	user	Not Specified							
dst <name>	Destination address name. Address or address group name.	string	Maximum length: 79							
dst-negate	Enable/disable negation of destination address match.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable destination address negation.		
	<i>disable</i>	Disable destination address negation.		
dst6 <name>	Destination address6 name. Address6 or address6 group name.	string	Maximum length: 79	
end-port	End destination port number.	integer	Minimum value: 65535 0 Maximum value: 65535	
end-src-port	End source port number.	integer	Minimum value: 65535 0 Maximum value: 65535	
fib-best-match-force	Enable/disable force using fib-best-match oif as outgoing interface.	option	-	disable
	Option Description			
	<i>disable</i>	Do not force using fib-best-match oif as outgoing interface.		
	<i>enable</i>	Force using fib-best-match oif as outgoing interface.		
gateway	Enable/disable SD-WAN service gateway.	option	-	disable
	Option Description			
	<i>enable</i>	Enable SD-WAN service gateway.		
	<i>disable</i>	Disable SD-WAN service gateway.		
groups <name>	User groups. Group name.	string	Maximum length: 79	
hash-mode	Hash algorithm for selected priority members for load balance mode.	option	-	round-robin
	Option Description			
	<i>round-robin</i>	All traffic are distributed to selected interfaces in equal portions and circular order.		
	<i>source-ip-based</i>	All traffic from a source IP is sent to the same interface.		
	<i>source-dest-ip-based</i>	All traffic from a source IP to a destination IP is sent to the same interface.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inbandwidth</i></td><td>All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.</td></tr><tr><td><i>outbandwidth</i></td><td>All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.</td></tr><tr><td><i>bibandwidth</i></td><td>All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.</td></tr></table>	Option	Description	<i>inbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.	<i>outbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.	<i>bibandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.			
	Option	Description										
	<i>inbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.										
	<i>outbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.										
<i>bibandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.											
health-check <name>	Health check list. Health check name.	string	Maximum length: 79									
hold-down-time	Waiting period in seconds when switching from the back-up member to the primary member (0 - 10000000, default = 0).	integer	Minimum value: 0 0 Maximum value: 10000000									
id	SD-WAN rule ID (1 - 4000).	integer	Minimum value: 0 1 Maximum value: 4000									
input-device <name>	Source interface name. Interface name.	string	Maximum length: 79									
input-device-negate	Enable/disable negation of input device match.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negation of input device match.</td></tr><tr><td><i>disable</i></td><td>Disable negation of input device match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negation of input device match.	<i>disable</i>	Disable negation of input device match.					
	Option	Description										
	<i>enable</i>	Enable negation of input device match.										
<i>disable</i>	Disable negation of input device match.											
input-zone <name>	Source input-zone name. Zone.	string	Maximum length: 79									
internet-service	Enable/disable use of Internet service for application-based load balancing.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable cloud service to support application-based load balancing.</td></tr><tr><td><i>disable</i></td><td>Disable cloud service to support application-based load balancing.</td></tr></table>	Option	Description	<i>enable</i>	Enable cloud service to support application-based load balancing.	<i>disable</i>	Disable cloud service to support application-based load balancing.					
	Option	Description										
	<i>enable</i>	Enable cloud service to support application-based load balancing.										
<i>disable</i>	Disable cloud service to support application-based load balancing.											
internet-service-app-ctrl <id>	Application control based Internet Service ID list. Application control based Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295									

Parameter	Description	Type	Size	Default														
internet-service-app-ctrl-category <id>	IDs of one or more application control categories. Application control category ID.	integer	Minimum value: 0 Maximum value: 4294967295															
internet-service-app-ctrl-group <name>	Application control based Internet Service group list. Application control based Internet Service group name.	string	Maximum length: 79															
internet-service-custom <name>	Custom Internet service name list. Custom Internet service name.	string	Maximum length: 79															
internet-service-custom-group <name>	Custom Internet Service group list. Custom Internet Service group name.	string	Maximum length: 79															
internet-service-group <name>	Internet Service group list. Internet Service group name.	string	Maximum length: 79															
internet-service-name <name>	Internet service name list. Internet service name.	string	Maximum length: 79															
jitter-weight	Coefficient of jitter in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000															
latency-weight	Coefficient of latency in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000															
link-cost-factor	Link cost factor.	option	-	latency														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>latency</td><td>Select link based on latency.</td></tr><tr><td>jitter</td><td>Select link based on jitter.</td></tr><tr><td>packet-loss</td><td>Select link based on packet loss.</td></tr><tr><td>inbandwidth</td><td>Select link based on available bandwidth of incoming traffic.</td></tr><tr><td>outbandwidth</td><td>Select link based on available bandwidth of outgoing traffic.</td></tr><tr><td>bibandwidth</td><td>Select link based on available bandwidth of bidirectional traffic.</td></tr></table>				Option	Description	latency	Select link based on latency.	jitter	Select link based on jitter.	packet-loss	Select link based on packet loss.	inbandwidth	Select link based on available bandwidth of incoming traffic.	outbandwidth	Select link based on available bandwidth of outgoing traffic.	bibandwidth	Select link based on available bandwidth of bidirectional traffic.
Option	Description																	
latency	Select link based on latency.																	
jitter	Select link based on jitter.																	
packet-loss	Select link based on packet loss.																	
inbandwidth	Select link based on available bandwidth of incoming traffic.																	
outbandwidth	Select link based on available bandwidth of outgoing traffic.																	
bibandwidth	Select link based on available bandwidth of bidirectional traffic.																	

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>custom-profile-1</i></td><td>Select link based on customized profile.</td></tr></table>	Option	Description	<i>custom-profile-1</i>	Select link based on customized profile.									
Option	Description													
<i>custom-profile-1</i>	Select link based on customized profile.													
link-cost-threshold	Percentage threshold change of link cost values that will result in policy route regeneration (0 - 10000000, default = 10).	integer	Minimum value: 0 Maximum value: 10000000	10										
load-balance	Enable/disable load-balance.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable load-balance.</td></tr><tr><td><i>disable</i></td><td>Disable load-balance.</td></tr></table>	Option	Description	<i>enable</i>	Enable load-balance.	<i>disable</i>	Disable load-balance.							
Option	Description													
<i>enable</i>	Enable load-balance.													
<i>disable</i>	Disable load-balance.													
minimum-sla-meet-members	Minimum number of members which meet SLA.	integer	Minimum value: 0 Maximum value: 255	0										
mode	Control how the SD-WAN rule sets the priority of interfaces in the SD-WAN.	option	-	manual										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Assign interfaces a priority based on quality.</td></tr><tr><td><i>manual</i></td><td>Assign interfaces a priority manually.</td></tr><tr><td><i>priority</i></td><td>Assign interfaces a priority based on the link-cost-factor quality of the interface.</td></tr><tr><td><i>sla</i></td><td>Assign interfaces a priority based on selected SLA settings.</td></tr></table>	Option	Description	<i>auto</i>	Assign interfaces a priority based on quality.	<i>manual</i>	Assign interfaces a priority manually.	<i>priority</i>	Assign interfaces a priority based on the link-cost-factor quality of the interface.	<i>sla</i>	Assign interfaces a priority based on selected SLA settings.			
Option	Description													
<i>auto</i>	Assign interfaces a priority based on quality.													
<i>manual</i>	Assign interfaces a priority manually.													
<i>priority</i>	Assign interfaces a priority based on the link-cost-factor quality of the interface.													
<i>sla</i>	Assign interfaces a priority based on selected SLA settings.													
name	SD-WAN rule name.	string	Maximum length: 35											
packet-loss-weight	Coefficient of packet-loss in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0										
passive-measurement	Enable/disable passive measurement based on the service criteria.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable passive measurement of user traffic.</td></tr><tr><td><i>disable</i></td><td>Disable passive measurement of user traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable passive measurement of user traffic.	<i>disable</i>	Disable passive measurement of user traffic.							
Option	Description													
<i>enable</i>	Enable passive measurement of user traffic.													
<i>disable</i>	Disable passive measurement of user traffic.													

Parameter	Description	Type	Size	Default								
priority-members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295									
priority-zone <name>	Priority zone name list. Priority zone name.	string	Maximum length: 79									
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255									
quality-link	Quality grade.	integer	Minimum value: 0 Maximum value: 255									
role	Service role to work with neighbor.	option	-	standalone								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standalone</i></td><td>Standalone service.</td></tr><tr><td><i>primary</i></td><td>Primary service for primary neighbor.</td></tr><tr><td><i>secondary</i></td><td>Secondary service for secondary neighbor.</td></tr></table>	Option	Description	<i>standalone</i>	Standalone service.	<i>primary</i>	Primary service for primary neighbor.	<i>secondary</i>	Secondary service for secondary neighbor.			
Option	Description											
<i>standalone</i>	Standalone service.											
<i>primary</i>	Primary service for primary neighbor.											
<i>secondary</i>	Secondary service for secondary neighbor.											
shortcut	Enable/disable shortcut for this service.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of ADVPN shortcut for this service.</td></tr><tr><td><i>disable</i></td><td>Disable use of ADVPN shortcut for this service.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of ADVPN shortcut for this service.	<i>disable</i>	Disable use of ADVPN shortcut for this service.					
Option	Description											
<i>enable</i>	Enable use of ADVPN shortcut for this service.											
<i>disable</i>	Disable use of ADVPN shortcut for this service.											
shortcut-priority	High priority of ADVPN shortcut for this service.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable a high priority of ADVPN shortcut for this service.</td></tr><tr><td><i>disable</i></td><td>Disable a high priority of ADVPN shortcut for this service.</td></tr><tr><td><i>auto</i></td><td>Auto enable a high priority of ADVPN shortcut for this service if ADVPN2.0 enabled.</td></tr></table>	Option	Description	<i>enable</i>	Enable a high priority of ADVPN shortcut for this service.	<i>disable</i>	Disable a high priority of ADVPN shortcut for this service.	<i>auto</i>	Auto enable a high priority of ADVPN shortcut for this service if ADVPN2.0 enabled.			
Option	Description											
<i>enable</i>	Enable a high priority of ADVPN shortcut for this service.											
<i>disable</i>	Disable a high priority of ADVPN shortcut for this service.											
<i>auto</i>	Auto enable a high priority of ADVPN shortcut for this service if ADVPN2.0 enabled.											
sla-compare-method	Method to compare SLA value for SLA mode.	option	-	order								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>order</i></td><td>Compare SLA value based on the order of health-check.</td></tr></table>	Option	Description	<i>order</i>	Compare SLA value based on the order of health-check.							
Option	Description											
<i>order</i>	Compare SLA value based on the order of health-check.											

Parameter	Description	Type	Size	Default
	Option Description			
	<i>number</i>	Compare SLA value based on the number of satisfied health-check. Limits health-checks to only configured member interfaces.		
sla-stickness	Enable/disable SLA stickiness (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Traffic remains in the original session path if the path is within the SLA.		
	<i>disable</i>	Traffic switches to the best path regardless of the SLA.		
src <name>	Source address name. Address or address group name.	string	Maximum length: 79	
src-negate	Enable/disable negation of source address match.	option	-	disable
	Option Description			
	<i>enable</i>	Enable source address negation.		
	<i>disable</i>	Disable source address negation.		
src6 <name>	Source address6 name. Address6 or address6 group name.	string	Maximum length: 79	
standalone-action	Enable/disable service when selected neighbor role is standalone while service role is not standalone.	option	-	disable
	Option Description			
	<i>enable</i>	Enable service when selected neighbor role is standalone.		
	<i>disable</i>	Disable service when selected neighbor role is standalone.		
start-port	Start destination port number.	integer	Minimum value: 1 0 Maximum value: 65535	
start-src-port	Start source port number.	integer	Minimum value: 1 0 Maximum value: 65535	
status	Enable/disable SD-WAN service.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable SD-WAN service.		
	<i>disable</i>	Disable SD-WAN service.		
tie-break	Method of selecting member if more than one meets the SLA.	option	-	zone
	Option	Description		
	<i>zone</i>	Use the setting that is configured for the members' zone.		
	<i>cfg-order</i>	Members that meet the SLA are selected in the order they are configured.		
	<i>fib-best-match</i>	Members that meet the SLA are selected that match the longest prefix in the routing table.		
	<i>input-device</i>	Members that meet the SLA are selected by matching the input device.		
tos	Type of service bit pattern.	user	Not Specified	
tos-mask	Type of service evaluated bits.	user	Not Specified	
use-shortcut-sla	Enable/disable use of ADVPN shortcut for quality comparison.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of ADVPN shortcut for quality comparison.		
	<i>disable</i>	Disable use of ADVPN shortcut for quality comparison.		
users <name>	User name. User name.	string	Maximum length: 79	
zone-mode	Enable/disable zone mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Traffic steered based on zone.		
	<i>disable</i>	Traffic steered based on member.		

config sla

Parameter	Description	Type	Size	Default
health-check	SD-WAN health-check.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
id	SLA ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0

config zone

Parameter	Description	Type	Size	Default								
advpn-health-check	Health check for ADVPN local overlay link quality.	string	Maximum length: 35									
advpn-select	Enable/disable selection of ADVPN based on SDWAN information.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable selection of ADVPN based on SDWAN information.</td></tr><tr><td>disable</td><td>Disable selection of ADVPN based on SDWAN information.</td></tr></table>				Option	Description	enable	Enable selection of ADVPN based on SDWAN information.	disable	Disable selection of ADVPN based on SDWAN information.		
Option	Description											
enable	Enable selection of ADVPN based on SDWAN information.											
disable	Disable selection of ADVPN based on SDWAN information.											
minimum-sla-meet-members	Minimum number of members which meet SLA when the neighbor is preferred.	integer	Minimum value: 1 Maximum value: 255	1								
name	Zone name.	string	Maximum length: 35									
service-sla-tie-break	Method of selecting member if more than one meets the SLA.	option	-	cfg-order								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cfg-order</td><td>Members that meet the SLA are selected in the order they are configured.</td></tr><tr><td>fib-best-match</td><td>Members that meet the SLA are selected that match the longest prefix in the routing table.</td></tr><tr><td>input-device</td><td>Members that meet the SLA are selected by matching the input device.</td></tr></table>				Option	Description	cfg-order	Members that meet the SLA are selected in the order they are configured.	fib-best-match	Members that meet the SLA are selected that match the longest prefix in the routing table.	input-device	Members that meet the SLA are selected by matching the input device.
Option	Description											
cfg-order	Members that meet the SLA are selected in the order they are configured.											
fib-best-match	Members that meet the SLA are selected that match the longest prefix in the routing table.											
input-device	Members that meet the SLA are selected by matching the input device.											

config system security-rating controls

Settings for individual Security Rating controls.

```
config system security-rating controls
  Description: Settings for individual Security Rating controls.
  edit <name>
```

```

    set display-insight [enable|disable]
    set display-report [enable|disable]
next
end

```

config system security-rating controls

Parameter	Description	Type	Size	Default						
display-insight	Enable/disable displaying the Security Rating control as an insight across the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable displaying the Security Rating control as an insight across the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable displaying the Security Rating control as an insight across the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable displaying the Security Rating control as an insight across the GUI.	<i>disable</i>	Disable displaying the Security Rating control as an insight across the GUI.			
Option	Description									
<i>enable</i>	Enable displaying the Security Rating control as an insight across the GUI.									
<i>disable</i>	Disable displaying the Security Rating control as an insight across the GUI.									
display-report	Enable/disable displaying the Security Rating control in the default report.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable displaying the Security Rating control in the default report.</td></tr><tr><td><i>disable</i></td><td>Disable displaying the Security Rating control in the default report.</td></tr></table>	Option	Description	<i>enable</i>	Enable displaying the Security Rating control in the default report.	<i>disable</i>	Disable displaying the Security Rating control in the default report.			
Option	Description									
<i>enable</i>	Enable displaying the Security Rating control in the default report.									
<i>disable</i>	Disable displaying the Security Rating control in the default report.									
name	Security Rating control name.	string	Maximum length: 35							

config system security-rating settings

Settings for Security Rating.

```

config system security-rating settings
    Description: Settings for Security Rating.
    set override-sync [enable|disable]
end

```


config system security-rating settings

Parameter	Description	Type	Size	Default						
override-sync	Enable/disable overriding Security Rating control settings synced from the Security Fabric's root FortiGate.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable overriding the Security Rating control settings synced from the Security Fabric root FortiGate.</td></tr><tr><td><i>disable</i></td><td>Disable overriding the Security Rating control settings synced from the Security Fabric root FortiGate.</td></tr></table>	Option	Description	<i>enable</i>	Enable overriding the Security Rating control settings synced from the Security Fabric root FortiGate.	<i>disable</i>	Disable overriding the Security Rating control settings synced from the Security Fabric root FortiGate.			
Option	Description									
<i>enable</i>	Enable overriding the Security Rating control settings synced from the Security Fabric root FortiGate.									
<i>disable</i>	Disable overriding the Security Rating control settings synced from the Security Fabric root FortiGate.									

config system serial-port



This command is available for model(s): FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Serial port list. Read-only.

```
config system serial-port
  Description: Serial port list. Read-only.
  edit <name>
```

```
next
end
```

config system serial-port

Parameter	Description	Type	Size	Default
name	Serial port name.	string	Maximum length: 35	

config system session-helper

Configure session helper.

```
config system session-helper
  Description: Configure session helper.
  edit <id>
    set name [ftp|tftp|...]
    set port {integer}
    set protocol {integer}
  next
end
```

config system session-helper

Parameter	Description	Type	Size	Default														
id	Session helper ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0														
name	Helper name.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>tftp</td><td>TFTP.</td></tr><tr><td>ras</td><td>RAS.</td></tr><tr><td>h323</td><td>H323.</td></tr><tr><td>tns</td><td>TNS.</td></tr><tr><td>mms</td><td>MMS.</td></tr></table>				Option	Description	ftp	FTP.	tftp	TFTP.	ras	RAS.	h323	H323.	tns	TNS.	mms	MMS.
	Option	Description																
	ftp	FTP.																
	tftp	TFTP.																
	ras	RAS.																
	h323	H323.																
	tns	TNS.																
mms	MMS.																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sip</i>	SIP.		
	<i>pptp</i>	PPTP.		
	<i>rtsp</i>	RTSP.		
	<i>dns-udp</i>	DNS UDP.		
	<i>dns-tcp</i>	DNS TCP.		
	<i>pmap</i>	PMAP.		
	<i>rsh</i>	RSH.		
	<i>dcerpc</i>	DCERPC.		
	<i>mgcp</i>	MGCP.		
port	Protocol port.	integer	Minimum value: 0 1 Maximum value: 65535	0
protocol	Protocol number.	integer	Minimum value: 0 0 Maximum value: 255	0

config system session-ttl

Configure global session TTL timers for this FortiGate.

```

config system session-ttl
  Description: Configure global session TTL timers for this FortiGate.
  set default {user}
  config port
    Description: Session TTL port.
    edit <id>
      set end-port {integer}
      set protocol {integer}
      set refresh-direction [both|outgoing|...]
      set start-port {integer}
      set timeout {user}
    next
  end
end
end

```

config system session-ttl

Parameter	Description	Type	Size	Default
default	Default timeout.	user	Not Specified	

config port

Parameter	Description	Type	Size	Default								
end-port	End port number.	integer	Minimum value: 0 Maximum value: 65535	0								
id	Table entry ID.	integer	Minimum value: 0 Maximum value: 65535	0								
protocol	Protocol (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0								
refresh-direction	Configure refresh direction.	option	-	both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>both</i></td><td>Refresh both directions.</td></tr><tr><td><i>outgoing</i></td><td>Refresh outgoing direction (original).</td></tr><tr><td><i>incoming</i></td><td>Refresh incoming direction (reply).</td></tr></table>				Option	Description	<i>both</i>	Refresh both directions.	<i>outgoing</i>	Refresh outgoing direction (original).	<i>incoming</i>	Refresh incoming direction (reply).
	Option	Description										
	<i>both</i>	Refresh both directions.										
	<i>outgoing</i>	Refresh outgoing direction (original).										
<i>incoming</i>	Refresh incoming direction (reply).											
start-port	Start port number.	integer	Minimum value: 0 Maximum value: 65535	0								
timeout	Session timeout (TTL).	user	Not Specified									

config system settings

Configure VDOM settings.

```
config system settings
  Description: Configure VDOM settings.
  set allow-linkdown-path [enable|disable]
  set allow-subnet-overlap [enable|disable]
  set asymroute [enable|disable]
  set asymroute-icmp [enable|disable]
  set asymroute6 [enable|disable]
  set asymroute6-icmp [enable|disable]
  set auxiliary-session [enable|disable]
  set bfd [enable|disable]
  set bfd-desired-min-tx {integer}
  set bfd-detect-mult {integer}
  set bfd-dont-enforce-src-port [enable|disable]
  set bfd-required-min-rx {integer}
  set block-land-attack [disable|enable]
  set central-nat [enable|disable]
  set comments {var-string}
  set default-app-port-as-service [enable|disable]
  set default-policy-expiry-days {integer}
  set default-voip-alg-mode [proxy-based|kernel-helper-based]
  set deny-tcp-with-icmp [enable|disable]
  set detect-unknown-esp [enable|disable]
  set device {string}
  set dhcp-proxy [enable|disable]
  set dhcp-proxy-interface {string}
  set dhcp-proxy-interface-select-method [auto|sdwan|...]
  set dhcp-proxy-vrf-select {integer}
  set dhcp-server-ip {user}
  set dhcp6-server-ip {user}
  set discovered-device-timeout {integer}
  set dyn-addr-session-check [enable|disable]
  set ecmp-max-paths {integer}
  set email-portal-check-dns [disable|enable]
  set ext-resource-session-check [enable|disable]
  set firewall-session-dirty [check-all|check-new|...]
  set fqdn-session-check [enable|disable]
  set fw-session-hairpin [enable|disable]
  set gateway {ipv4-address}
  set gateway6 {ipv6-address}
  set gui-advanced-policy [enable|disable]
  set gui-advanced-wireless-features [enable|disable]
  set gui-allow-unnamed-policy [enable|disable]
  set gui-antivirus [enable|disable]
  set gui-ap-profile [enable|disable]
  set gui-application-control [enable|disable]
  set gui-casb [enable|disable]
  set gui-default-policy-columns <name1>, <name2>, ...
  set gui-dhcp-advanced [enable|disable]
  set gui-dlp-advanced [enable|disable]
  set gui-dlp-profile [enable|disable]
  set gui-dns-database [enable|disable]
  set gui-dnsfilter [enable|disable]
```

```
set gui-dos-policy [enable|disable]
set gui-dynamic-device-os-id [enable|disable]
set gui-dynamic-routing [enable|disable]
set gui-email-collection [enable|disable]
set gui-enforce-change-summary [disable|require|...]
set gui-explicit-proxy [enable|disable]
set gui-file-filter [enable|disable]
set gui-fortiap-split-tunneling [enable|disable]
set gui-fortiextender-controller [enable|disable]
set gui-fortitelemetry [enable|disable]
set gui-gtp [enable|disable]
set gui-icap [enable|disable]
set gui-implicit-policy [enable|disable]
set gui-ips [enable|disable]
set gui-load-balance [enable|disable]
set gui-local-in-policy [enable|disable]
set gui-multicast-policy [enable|disable]
set gui-multiple-interface-policy [enable|disable]
set gui-object-colors [enable|disable]
set gui-ot [enable|disable]
set gui-policy-based-ipsec [enable|disable]
set gui-policy-disclaimer [enable|disable]
set gui-route-tag-address-creation [enable|disable]
set gui-security-profile-group [enable|disable]
set gui-spamfilter [enable|disable]
set gui-sslvpn [enable|disable]
set gui-sslvpn-personal-bookmarks [enable|disable]
set gui-sslvpn-realms [enable|disable]
set gui-switch-controller [enable|disable]
set gui-threat-weight [enable|disable]
set gui-traffic-shaping [enable|disable]
set gui-videofilter [enable|disable]
set gui-virtual-patch-profile [enable|disable]
set gui-voip-profile [enable|disable]
set gui-vpn [enable|disable]
set gui-waf-profile [enable|disable]
set gui-wan-load-balancing [enable|disable]
set gui-wanopt-cache [enable|disable]
set gui-webfilter [enable|disable]
set gui-webfilter-advanced [enable|disable]
set gui-wireless-controller [enable|disable]
set gui-ztna [enable|disable]
set h323-direct-model [disable|enable]
set http-external-dest [fortiweb|forticache]
set ike-detailed-event-logs [disable|enable]
set ike-dn-format [with-space|no-space]
set ike-policy-route [enable|disable]
set ike-port {integer}
set ike-quick-crash-detect [enable|disable]
set ike-session-resume [enable|disable]
set ike-tcp-port {integer}
set internet-service-app-ctrl-size {integer}
```

```

set internet-service-database-cache [disable|enable]
set intree-ses-best-route [force|disable]
set ip {ipv4-classnet-host}
set ip6 {ipv6-prefix}
set lan-extension-controller-addr {string}
set link-down-access [enable|disable]
set lldp-reception [enable|disable|...]
set lldp-transmission [enable|disable|...]
set location-id {ipv4-address}
set mac-ttl {integer}
set manageip {user}
set manageip6 {ipv6-prefix}
set multicast-forward [enable|disable]
set multicast-skip-policy [enable|disable]
set multicast-ttl-notchchange [enable|disable]
set nat46-force-ipv4-packet-forwarding [enable|disable]
set nat46-generate-ipv6-fragment-header [enable|disable]
set nat64-force-ipv6-packet-forwarding [enable|disable]
set ngfw-mode [profile-based|policy-based]
set opmode [nat|transparent]
set policy-offload-level [disable|dos-offload]
set prp-trailer-action [enable|disable]
set sccp-port {integer}
set sctp-session-without-init [enable|disable]
set ses-denied-multicast-traffic [enable|disable]
set ses-denied-traffic [enable|disable]
set sip-expectation [enable|disable]
set sip-nat-trace [enable|disable]
set sip-ssl-port {integer}
set sip-tcp-port {integer}
set sip-udp-port {integer}
set snat-hairpin-traffic [enable|disable]
set status [enable|disable]
set strict-src-check [enable|disable]
set tcp-session-without-syn [enable|disable]
set utf8-spam-tagging [enable|disable]
set v4-ecmp-mode [source-ip-based|weight-based|...]
set vdom-type [traffic|lan-extension|...]
set vpn-stats-log {option1}, {option2}, ...
set vpn-stats-period {integer}
set wccp-cache-engine [enable|disable]

end

```

config system settings

Parameter	Description	Type	Size	Default
allow-linkdown-path	Enable/disable link down path.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Allow link down path.		
	<i>disable</i>	Do not allow link down path.		
allow-subnet-overlap	Enable/disable allowing interface subnets to use overlapping IP addresses.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable overlapping subnets.		
	<i>disable</i>	Disable overlapping subnets.		
asymroute	Enable/disable IPv4 asymmetric routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPv4 asymmetric routing.		
	<i>disable</i>	Disable IPv4 asymmetric routing.		
asymroute-icmp	Enable/disable ICMP asymmetric routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ICMP asymmetric routing.		
	<i>disable</i>	Disable ICMP asymmetric routing.		
asymroute6	Enable/disable asymmetric IPv6 routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable asymmetric IPv6 routing.		
	<i>disable</i>	Disable asymmetric IPv6 routing.		
asymroute6-icmp	Enable/disable asymmetric ICMPv6 routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable asymmetric ICMPv6 routing.		
	<i>disable</i>	Disable asymmetric ICMPv6 routing.		
auxiliary-session	Enable/disable auxiliary session.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable auxiliary session for this VDOM.		
	<i>disable</i>	Disable auxiliary session for this VDOM.		
bfd	Enable/disable Bi-directional Forwarding Detection (BFD) on all interfaces.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Bi-directional Forwarding Detection (BFD) on all interfaces.		
	<i>disable</i>	Disable Bi-directional Forwarding Detection (BFD) on all interfaces.		
bfd-desired-min-tx	BFD desired minimal transmit interval (1 - 100000 ms, default = 250).	integer	Minimum value: 250 1 Maximum value: 100000	
bfd-detect-mult	BFD detection multiplier (1 - 50, default = 3).	integer	Minimum value: 3 1 Maximum value: 50	
bfd-dont-enforce-src-port	Enable to not enforce verifying the source port of BFD Packets.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable verifying the source port of BFD Packets.		
	<i>disable</i>	Disable verifying the source port of BFD Packets.		
bfd-required-min-rx	BFD required minimal receive interval (1 - 100000 ms, default = 250).	integer	Minimum value: 250 1 Maximum value: 100000	
block-land-attack	Enable/disable blocking of land attacks.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not block land attack.		
	<i>enable</i>	Block land attack.		
central-nat	Enable/disable central NAT.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable central NAT.		
	<i>disable</i>	Disable central NAT.		

Parameter	Description	Type	Size	Default						
comments	VDOM comments.	var-string	Maximum length: 255							
default-app-port-as-service	Enable/disable policy service enforcement based on application default ports.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-policy-expiry-days	Default policy expiry in days (0 - 365 days, default = 30).	integer	Minimum value: 0 Maximum value: 365	30						
default-voip-alg-mode	Configure how the FortiGate handles VoIP traffic when a policy that accepts the traffic doesn't include a VoIP profile.	option	-	proxy-based						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>proxy-based</i></td><td>Use a default proxy-based VoIP ALG.</td></tr><tr><td><i>kernel-helper-based</i></td><td>Use the SIP session helper.</td></tr></table>	Option	Description	<i>proxy-based</i>	Use a default proxy-based VoIP ALG.	<i>kernel-helper-based</i>	Use the SIP session helper.			
Option	Description									
<i>proxy-based</i>	Use a default proxy-based VoIP ALG.									
<i>kernel-helper-based</i>	Use the SIP session helper.									
deny-tcp-with-icmp	Enable/disable denying TCP by sending an ICMP communication prohibited packet.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Deny TCP with ICMP.</td></tr><tr><td><i>disable</i></td><td>Disable denying TCP with ICMP.</td></tr></table>	Option	Description	<i>enable</i>	Deny TCP with ICMP.	<i>disable</i>	Disable denying TCP with ICMP.			
Option	Description									
<i>enable</i>	Deny TCP with ICMP.									
<i>disable</i>	Disable denying TCP with ICMP.									
detect-unknown-esp	Enable/disable detection of unknown ESP packets (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable detection of unknown ESP packets and drop the ESP packet if it's unknown.</td></tr><tr><td><i>disable</i></td><td>Disable detection of unknown ESP packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable detection of unknown ESP packets and drop the ESP packet if it's unknown.	<i>disable</i>	Disable detection of unknown ESP packets.			
Option	Description									
<i>enable</i>	Enable detection of unknown ESP packets and drop the ESP packet if it's unknown.									
<i>disable</i>	Disable detection of unknown ESP packets.									
device	Interface to use for management access for NAT mode.	string	Maximum length: 35							
dhcp-proxy	Enable/disable the DHCP Proxy.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the DHCP proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the DHCP proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable the DHCP proxy.	<i>disable</i>	Disable the DHCP proxy.					
	Option	Description										
	<i>enable</i>	Enable the DHCP proxy.										
<i>disable</i>	Disable the DHCP proxy.											
dhcp-proxy-interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
dhcp-proxy-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
dhcp-proxy-vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511									
dhcp-server-ip	DHCP Server IPv4 address.	user	Not Specified									
dhcp6-server-ip	DHCPv6 server IPv6 address.	user	Not Specified									
discovered-device-timeout	Timeout for discovered devices (1 - 365 days, default = 28).	integer	Minimum value: 1 Maximum value: 365	28								
dyn-addr-session-check	Enable/disable dirty session check caused by dynamic address updates.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dirty session check caused by dynamic address updates.</td></tr><tr><td><i>disable</i></td><td>Disable dirty session check caused by dynamic address updates.</td></tr></table>	Option	Description	<i>enable</i>	Enable dirty session check caused by dynamic address updates.	<i>disable</i>	Disable dirty session check caused by dynamic address updates.					
	Option	Description										
	<i>enable</i>	Enable dirty session check caused by dynamic address updates.										
<i>disable</i>	Disable dirty session check caused by dynamic address updates.											
ecmp-max-paths	Maximum number of Equal Cost Multi-Path (ECMP) next-hops. Set to 1 to disable ECMP routing (1 - 255, default = 255).	integer	Minimum value: 1 Maximum value: 255	255								
email-portal-check-dns	Enable/disable using DNS to validate email addresses collected by a captive portal.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable email address checking with DNS.</td></tr><tr><td><i>enable</i></td><td>Enable email address checking with DNS.</td></tr></table>	Option	Description	<i>disable</i>	Disable email address checking with DNS.	<i>enable</i>	Enable email address checking with DNS.					
	Option	Description										
	<i>disable</i>	Disable email address checking with DNS.										
<i>enable</i>	Enable email address checking with DNS.											

Parameter	Description	Type	Size	Default								
ext-resource-session-check	Enable/disable dirty session check caused by external resource updates.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dirty session check caused by external resource updates.</td></tr><tr><td>disable</td><td>Disable dirty session check caused by external resource updates.</td></tr></table>	Option	Description	enable	Enable dirty session check caused by external resource updates.	disable	Disable dirty session check caused by external resource updates.					
Option	Description											
enable	Enable dirty session check caused by external resource updates.											
disable	Disable dirty session check caused by external resource updates.											
firewall-session-dirty	Select how to manage sessions affected by firewall policy configuration changes.	option	-	check-all								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>check-all</td><td>All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.</td></tr><tr><td>check-new</td><td>Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.</td></tr><tr><td>check-policy-option</td><td>Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.</td></tr></table>	Option	Description	check-all	All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.	check-new	Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.	check-policy-option	Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.			
Option	Description											
check-all	All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.											
check-new	Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.											
check-policy-option	Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.											
fqdn-session-check	Enable/disable dirty session check caused by FQDN updates.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dirty session check caused by FQDN updates.</td></tr><tr><td>disable</td><td>Disable dirty session check caused by FQDN updates.</td></tr></table>	Option	Description	enable	Enable dirty session check caused by FQDN updates.	disable	Disable dirty session check caused by FQDN updates.					
Option	Description											
enable	Enable dirty session check caused by FQDN updates.											
disable	Disable dirty session check caused by FQDN updates.											
fw-session-hairpin	Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiGate.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Perform a policy check every time.</td></tr><tr><td>disable</td><td>Perform a policy check only the first time the session is received.</td></tr></table>	Option	Description	enable	Perform a policy check every time.	disable	Perform a policy check only the first time the session is received.					
Option	Description											
enable	Perform a policy check every time.											
disable	Perform a policy check only the first time the session is received.											
gateway	Transparent mode IPv4 default gateway IP address.	ipv4-address	Not Specified	0.0.0.0								
gateway6	Transparent mode IPv6 default gateway IP address.	ipv6-address	Not Specified	::								
gui-advanced-policy	Enable/disable advanced policy configuration on the GUI.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable advanced policy configuration on the GUI.		
	<i>disable</i>	Disable advanced policy configuration on the GUI.		
gui-advanced-wireless-features	Enable/disable advanced wireless features in GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable advanced wireless features in GUI.		
	<i>disable</i>	Disable advanced wireless features in GUI.		
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the requirement for policy naming on the GUI.		
	<i>disable</i>	Disable the requirement for policy naming on the GUI.		
gui-antivirus	Enable/disable AntiVirus on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable AntiVirus on the GUI.		
	<i>disable</i>	Disable AntiVirus on the GUI.		
gui-ap-profile	Enable/disable FortiAP profiles on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiAP profiles on the GUI.		
	<i>disable</i>	Disable FortiAP profiles on the GUI.		
gui-application-control	Enable/disable application control on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable application control on the GUI.		
	<i>disable</i>	Disable application control on the GUI.		
gui-casb	Enable/disable Inline-CASB on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable Inline-CASB on the GUI.		
	<i>disable</i>	Disable Inline-CASB on the GUI.		
gui-default-policy-columns <name>	Default columns to display for policy lists on GUI. Select column name.	string	Maximum length: 79	
gui-dhcp-advanced	Enable/disable advanced DHCP options on the GUI.	option	-	enable
	Option Description			
	<i>enable</i>	Enable advanced DHCP options on the GUI.		
	<i>disable</i>	Disable advanced DHCP options on the GUI.		
gui-dlp-advanced	Enable/disable Show advanced DLP expressions on the GUI.	option	-	disable
	Option Description			
	<i>enable</i>	Enable Show advanced DLP expressions on the GUI.		
	<i>disable</i>	Disable Show advanced DLP expressions on the GUI.		
gui-dlp-profile	Enable/disable Data Loss Prevention on the GUI.	option	-	disable
	Option Description			
	<i>enable</i>	Enable Data Loss Prevention on the GUI.		
	<i>disable</i>	Disable Data Loss Prevention on the GUI.		
gui-dns-database	Enable/disable DNS database settings on the GUI.	option	-	disable
	Option Description			
	<i>enable</i>	Enable DNS database settings on the GUI.		
	<i>disable</i>	Disable DNS database settings on the GUI.		
gui-dnsfilter	Enable/disable DNS Filtering on the GUI.	option	-	enable
	Option Description			
	<i>enable</i>	Enable DNS Filtering on the GUI.		
	<i>disable</i>	Disable DNS Filtering on the GUI.		

Parameter	Description	Type	Size	Default								
gui-dos-policy	Enable/disable DoS policies on the GUI.	option	-	enable **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DoS policies on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable DoS policies on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DoS policies on the GUI.	<i>disable</i>	Disable DoS policies on the GUI.					
Option	Description											
<i>enable</i>	Enable DoS policies on the GUI.											
<i>disable</i>	Disable DoS policies on the GUI.											
gui-dynamic-device-os-id	Enable/disable Create dynamic addresses to manage known devices.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Create dynamic addresses to manage known devices.</td></tr><tr><td><i>disable</i></td><td>Disable Create dynamic addresses to manage known devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable Create dynamic addresses to manage known devices.	<i>disable</i>	Disable Create dynamic addresses to manage known devices.					
Option	Description											
<i>enable</i>	Enable Create dynamic addresses to manage known devices.											
<i>disable</i>	Disable Create dynamic addresses to manage known devices.											
gui-dynamic-routing	Enable/disable dynamic routing on the GUI.	option	-	enable **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic routing on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic routing on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic routing on the GUI.	<i>disable</i>	Disable dynamic routing on the GUI.					
Option	Description											
<i>enable</i>	Enable dynamic routing on the GUI.											
<i>disable</i>	Disable dynamic routing on the GUI.											
gui-email-collection	Enable/disable email collection on the GUI.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable email collection on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable email collection on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable email collection on the GUI.	<i>disable</i>	Disable email collection on the GUI.					
Option	Description											
<i>enable</i>	Enable email collection on the GUI.											
<i>disable</i>	Disable email collection on the GUI.											
gui-enforce-change-summary	Enforce change summaries for select tables in the GUI.	option	-	require								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>No change summary requirement.</td></tr><tr><td><i>require</i></td><td>Change summary required.</td></tr><tr><td><i>optional</i></td><td>Change summary optional.</td></tr></table>	Option	Description	<i>disable</i>	No change summary requirement.	<i>require</i>	Change summary required.	<i>optional</i>	Change summary optional.			
Option	Description											
<i>disable</i>	No change summary requirement.											
<i>require</i>	Change summary required.											
<i>optional</i>	Change summary optional.											
gui-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the explicit proxy on the GUI.		
	<i>disable</i>	Disable the explicit proxy on the GUI.		
gui-file-filter	Enable/disable File-filter on the GUI.	option	-	enable **
	Option	Description		
	<i>enable</i>	Enable File-filter on the GUI.		
	<i>disable</i>	Disable File-filter on the GUI.		
gui-fortiap-split-tunneling	Enable/disable FortiAP split tunneling on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiAP split tunneling on the GUI.		
	<i>disable</i>	Disable FortiAP split tunneling on the GUI.		
gui-fortitender-controller	Enable/disable FortiExtender on the GUI.	option	-	disable **
	Option	Description		
	<i>enable</i>	Enable FortiExtender on the GUI.		
	<i>disable</i>	Disable FortiExtender on the GUI.		
gui-fortitelemetry *	Enable/disable FortiTelemetry on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiTelemetry on the GUI.		
	<i>disable</i>	Disable FortiTelemetry on the GUI.		
gui-gtp *	Enable/disable Manage general radio packet service (GPRS) protocols on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Manage general radio packet service (GPRS) protocols on the GUI.		
	<i>disable</i>	Disable Manage general radio packet service (GPRS) protocols on the GUI.		

Parameter	Description	Type	Size	Default						
gui-icap	Enable/disable ICAP on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ICAP on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable ICAP on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable ICAP on the GUI.	<i>disable</i>	Disable ICAP on the GUI.			
Option	Description									
<i>enable</i>	Enable ICAP on the GUI.									
<i>disable</i>	Disable ICAP on the GUI.									
gui-implicit-policy	Enable/disable implicit firewall policies on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable implicit firewall policies on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable implicit firewall policies on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable implicit firewall policies on the GUI.	<i>disable</i>	Disable implicit firewall policies on the GUI.			
Option	Description									
<i>enable</i>	Enable implicit firewall policies on the GUI.									
<i>disable</i>	Disable implicit firewall policies on the GUI.									
gui-ips	Enable/disable IPS on the GUI.	option	-	enable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable IPS on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS on the GUI.	<i>disable</i>	Disable IPS on the GUI.			
Option	Description									
<i>enable</i>	Enable IPS on the GUI.									
<i>disable</i>	Disable IPS on the GUI.									
gui-load-balance	Enable/disable server load balancing on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server load balancing on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable server load balancing on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable server load balancing on the GUI.	<i>disable</i>	Disable server load balancing on the GUI.			
Option	Description									
<i>enable</i>	Enable server load balancing on the GUI.									
<i>disable</i>	Disable server load balancing on the GUI.									
gui-local-in-policy	Enable/disable Local-In policies on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Local-In policies on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable Local-In policies on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable Local-In policies on the GUI.	<i>disable</i>	Disable Local-In policies on the GUI.			
Option	Description									
<i>enable</i>	Enable Local-In policies on the GUI.									
<i>disable</i>	Disable Local-In policies on the GUI.									
gui-multicast-policy	Enable/disable multicast firewall policies on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast firewall policies on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable multicast firewall policies on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast firewall policies on the GUI.	<i>disable</i>	Disable multicast firewall policies on the GUI.			
Option	Description									
<i>enable</i>	Enable multicast firewall policies on the GUI.									
<i>disable</i>	Disable multicast firewall policies on the GUI.									

Parameter	Description	Type	Size	Default						
gui-multiple-interface-policy	Enable/disable adding multiple interfaces to a policy on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adding multiple interfaces to a policy on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable adding multiple interfaces to a policy on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable adding multiple interfaces to a policy on the GUI.	<i>disable</i>	Disable adding multiple interfaces to a policy on the GUI.			
Option	Description									
<i>enable</i>	Enable adding multiple interfaces to a policy on the GUI.									
<i>disable</i>	Disable adding multiple interfaces to a policy on the GUI.									
gui-object-colors	Enable/disable object colors on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable object colors on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable object colors on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable object colors on the GUI.	<i>disable</i>	Disable object colors on the GUI.			
Option	Description									
<i>enable</i>	Enable object colors on the GUI.									
<i>disable</i>	Disable object colors on the GUI.									
gui-ot	Enable/disable Operational technology features on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Operational technology features on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable Operational technology features on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable Operational technology features on the GUI.	<i>disable</i>	Disable Operational technology features on the GUI.			
Option	Description									
<i>enable</i>	Enable Operational technology features on the GUI.									
<i>disable</i>	Disable Operational technology features on the GUI.									
gui-policy-based-ipsec	Enable/disable policy-based IPsec VPN on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy-based IPsec VPN on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable policy-based IPsec VPN on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy-based IPsec VPN on the GUI.	<i>disable</i>	Disable policy-based IPsec VPN on the GUI.			
Option	Description									
<i>enable</i>	Enable policy-based IPsec VPN on the GUI.									
<i>disable</i>	Disable policy-based IPsec VPN on the GUI.									
gui-policy-disclaimer	Enable/disable policy disclaimer on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy disclaimer on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable policy disclaimer on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy disclaimer on the GUI.	<i>disable</i>	Disable policy disclaimer on the GUI.			
Option	Description									
<i>enable</i>	Enable policy disclaimer on the GUI.									
<i>disable</i>	Disable policy disclaimer on the GUI.									
gui-route-tag-address-creation	Enable/disable route-tag addresses on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable route-tag addresses on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable route-tag addresses on the GUI.					
Option	Description									
<i>enable</i>	Enable route-tag addresses on the GUI.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable route-tag addresses on the GUI.		
gui-security-profile-group	Enable/disable Security Profile Groups on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Security Profile Groups on the GUI.		
	<i>disable</i>	Disable Security Profile Groups on the GUI.		
gui-spamfilter	Enable/disable Antispam on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Antispam on the GUI.		
	<i>disable</i>	Disable Antispam on the GUI.		
gui-sslvpn *	Enable/disable SSL-VPN settings pages on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-VPN settings pages on the GUI.		
	<i>disable</i>	Disable SSL-VPN settings pages on the GUI.		
gui-sslvpn-personal-bookmarks *	Enable/disable SSL-VPN personal bookmark management on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-VPN personal bookmark management on the GUI.		
	<i>disable</i>	Disable SSL-VPN personal bookmark management on the GUI.		
gui-sslvpn-realms *	Enable/disable SSL-VPN realms on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-VPN realms on the GUI.		
	<i>disable</i>	Disable SSL-VPN realms on the GUI.		
gui-switch-controller *	Enable/disable the switch controller on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the switch controller on the GUI.		
	<i>disable</i>	Disable the switch controller on the GUI.		
gui-threat-weight	Enable/disable threat weight on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable threat weight on the GUI.		
	<i>disable</i>	Disable threat weight on the GUI.		
gui-traffic-shaping	Enable/disable traffic shaping on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable traffic shaping on the GUI.		
	<i>disable</i>	Disable traffic shaping on the GUI.		
gui-videofilter	Enable/disable Video filtering on the GUI.	option	-	enable **
	Option	Description		
	<i>enable</i>	Enable Video filtering on the GUI.		
	<i>disable</i>	Disable Video filtering on the GUI.		
gui-virtual-patch-profile	Enable/disable Virtual Patching on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Virtual Patching on the GUI.		
	<i>disable</i>	Disable Virtual Patching on the GUI.		
gui-voip-profile	Enable/disable VoIP profiles on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable VoIP profiles on the GUI.		
	<i>disable</i>	Disable VoIP profiles on the GUI.		
gui-vpn	Enable/disable IPsec VPN settings pages on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable IPsec VPN settings pages on the GUI.		
	<i>disable</i>	Disable IPsec VPN settings pages on the GUI.		
gui-waf-profile	Enable/disable Web Application Firewall on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Web Application Firewall on the GUI.		
	<i>disable</i>	Disable Web Application Firewall on the GUI.		
gui-wan-load-balancing	Enable/disable SD-WAN on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable SD-WAN on the GUI.		
	<i>disable</i>	Disable SD-WAN on the GUI.		
gui-wanopt-cache *	Enable/disable WAN Optimization and Web Caching on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization and Web Caching on the GUI.		
	<i>disable</i>	Disable WAN Optimization and Web Caching on the GUI.		
gui-webfilter	Enable/disable Web filtering on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Web filtering on the GUI.		
	<i>disable</i>	Disable Web filtering on the GUI.		
gui-webfilter-advanced	Enable/disable advanced web filtering on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable advanced web filtering on the GUI.		
	<i>disable</i>	Disable advanced web filtering on the GUI.		
gui-wireless-controller	Enable/disable the wireless controller on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the wireless controller on the GUI.		
	<i>disable</i>	Disable the wireless controller on the GUI.		
gui-ztna	Enable/disable Zero Trust Network Access features on the GUI.	option	-	enable **
	Option	Description		
	<i>enable</i>	Enable Zero Trust Network Access features on the GUI.		
	<i>disable</i>	Disable Zero Trust Network Access features on the GUI.		
h323-direct-model	Enable/disable H323 direct model.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable H323 direct model.		
	<i>enable</i>	Enable H323 direct model.		
http-external-dest	Offload HTTP traffic to FortiWeb or FortiCache.	option	-	fortiweb
	Option	Description		
	<i>fortiweb</i>	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.		
	<i>forticache</i>	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.		
ike-detailed-event-logs	Enable/disable detail log for IKE events.	option	-	disable
	Option	Description		
	<i>disable</i>	Generate brief log for IKE events.		
	<i>enable</i>	Generate detail log for IKE events.		
ike-dn-format	Configure IKE ASN.1 Distinguished Name format conventions.	option	-	with-space
	Option	Description		
	<i>with-space</i>	Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-space</i></td><td>Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.</td></tr></table>	Option	Description	<i>no-space</i>	Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.					
	Option	Description								
<i>no-space</i>	Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.									
ike-policy-route	Enable/disable IKE Policy Based Routing (PBR).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKE Policy Based Routing (PBR).</td></tr><tr><td><i>disable</i></td><td>Disable IKE Policy Based Routing (PBR).</td></tr></table>	Option	Description	<i>enable</i>	Enable IKE Policy Based Routing (PBR).	<i>disable</i>	Disable IKE Policy Based Routing (PBR).			
	Option	Description								
	<i>enable</i>	Enable IKE Policy Based Routing (PBR).								
<i>disable</i>	Disable IKE Policy Based Routing (PBR).									
ike-port	UDP port for IKE/IPsec traffic (default 500).	integer	Minimum value: 500 1024 Maximum value: 65535							
ike-quick-crash-detect	Enable/disable IKE quick crash detection (RFC 6290).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKE quick crash detection (RFC 6290).</td></tr><tr><td><i>disable</i></td><td>Disable IKE quick crash detection (RFC 6290).</td></tr></table>	Option	Description	<i>enable</i>	Enable IKE quick crash detection (RFC 6290).	<i>disable</i>	Disable IKE quick crash detection (RFC 6290).			
	Option	Description								
	<i>enable</i>	Enable IKE quick crash detection (RFC 6290).								
<i>disable</i>	Disable IKE quick crash detection (RFC 6290).									
ike-session-resume	Enable/disable IKEv2 session resumption (RFC 5723).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 session resumption (RFC 5723).</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 session resumption (RFC 5723).</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 session resumption (RFC 5723).	<i>disable</i>	Disable IKEv2 session resumption (RFC 5723).			
	Option	Description								
	<i>enable</i>	Enable IKEv2 session resumption (RFC 5723).								
<i>disable</i>	Disable IKEv2 session resumption (RFC 5723).									
ike-tcp-port	TCP port for IKE/IPsec traffic (default 443).	integer	Minimum value: 443 1 Maximum value: 65535							
internet-service-app-ctrl-size	Maximum number of tuple entries (protocol, port, IP address, application ID) stored by the FortiGate unit (0 - 4294967295, default = 32768). A smaller value limits the FortiGate unit from learning about internet applications.	integer	Minimum value: 32768 0 Maximum value: 4294967295							
internet-service-database-cache	Enable/disable Internet Service database caching.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable Internet Service database caching.		
	<i>enable</i>	Enable Internet Service database caching.		
intree-ses-best-route	Force the intree session to always use the best route.	option	-	disable
	Option	Description		
	<i>force</i>	Force the intree session to always use the best route.		
	<i>disable</i>	Don't force the intree session to always use the best route.		
ip	IP address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
ip6	IPv6 address prefix for NAT mode.	ipv6-prefix	Not Specified	::/0
lan-extension-controller-addr	Controller IP address or FQDN to connect.	string	Maximum length: 255	
link-down-access	Enable/disable link down access traffic.	option	-	enable
	Option	Description		
	<i>enable</i>	Allow link down access traffic.		
	<i>disable</i>	Block link down access traffic.		
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception for this VDOM or apply global settings to this VDOM.	option	-	global
	Option	Description		
	<i>enable</i>	Enable LLDP reception for this VDOM.		
	<i>disable</i>	Disable LLDP reception for this VDOM.		
	<i>global</i>	Use the global LLDP reception configuration for this VDOM.		
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission for this VDOM or apply global settings to this VDOM.	option	-	global
	Option	Description		
	<i>enable</i>	Enable LLDP transmission for this VDOM.		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable LLDP transmission for this VDOM.		
	<i>global</i>	Use the global LLDP transmission configuration for this VDOM.		
location-id	Local location ID in the form of an IPv4 address.	ipv4-address	Not Specified	0.0.0.0
mac-ttl	Duration of MAC addresses in Transparent mode (300 - 8640000 sec, default = 300).	integer	Minimum value: 300 Maximum value: 8640000	300
manageip	Transparent mode IPv4 management IP address and netmask.	user	Not Specified	
manageip6	Transparent mode IPv6 management IP address and netmask.	ipv6-prefix	Not Specified	::/0
multicast-forward	Enable/disable multicast forwarding.	option	-	enable
	Option Description			
	<i>enable</i>	Enable multicast forwarding.		
	<i>disable</i>	Disable multicast forwarding.		
multicast-skip-policy	Enable/disable allowing multicast traffic through the FortiGate without a policy check.	option	-	disable
	Option Description			
	<i>enable</i>	Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.		
	<i>disable</i>	Require a multicast policy to allow multicast traffic to pass through the FortiGate.		
multicast-ttl-notchange	Enable/disable preventing the FortiGate from changing the TTL for forwarded multicast packets.	option	-	disable
	Option Description			
	<i>enable</i>	The multicast TTL is not changed.		
	<i>disable</i>	The multicast TTL may be changed.		

Parameter	Description	Type	Size	Default						
nat46-force-ipv4-packet-forwarding	Enable/disable mandatory IPv4 packet forwarding in NAT46.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.</td></tr><tr><td>disable</td><td>Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.</td></tr></table>	Option	Description	enable	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.	disable	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.			
Option	Description									
enable	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.									
disable	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.									
nat46-generate-ipv6-fragment-header	Enable/disable NAT46 IPv6 fragment header generation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NAT46 IPv6 fragment header generation.</td></tr><tr><td>disable</td><td>Disable NAT46 IPv6 fragment header generation.</td></tr></table>	Option	Description	enable	Enable NAT46 IPv6 fragment header generation.	disable	Disable NAT46 IPv6 fragment header generation.			
Option	Description									
enable	Enable NAT46 IPv6 fragment header generation.									
disable	Disable NAT46 IPv6 fragment header generation.									
nat64-force-ipv6-packet-forwarding	Enable/disable mandatory IPv6 packet forwarding in NAT64.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable mandatory IPv6 packet forwarding</td></tr><tr><td>disable</td><td>Disable mandatory IPv6 packet forwarding</td></tr></table>	Option	Description	enable	Enable mandatory IPv6 packet forwarding	disable	Disable mandatory IPv6 packet forwarding			
Option	Description									
enable	Enable mandatory IPv6 packet forwarding									
disable	Disable mandatory IPv6 packet forwarding									
ngfw-mode	Next Generation Firewall (NGFW) mode.	option	-	profile-based						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>profile-based</td><td>Application and web-filtering are configured using profiles applied to policy entries.</td></tr><tr><td>policy-based</td><td>Application and web-filtering are configured as policy match conditions.</td></tr></table>	Option	Description	profile-based	Application and web-filtering are configured using profiles applied to policy entries.	policy-based	Application and web-filtering are configured as policy match conditions.			
Option	Description									
profile-based	Application and web-filtering are configured using profiles applied to policy entries.									
policy-based	Application and web-filtering are configured as policy match conditions.									
opmode	Firewall operation mode (NAT or Transparent).	option	-	nat						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>nat</td><td>Change to NAT mode.</td></tr><tr><td>transparent</td><td>Change to transparent mode.</td></tr></table>	Option	Description	nat	Change to NAT mode.	transparent	Change to transparent mode.			
Option	Description									
nat	Change to NAT mode.									
transparent	Change to transparent mode.									

Parameter	Description	Type	Size	Default
policy-offload-level *	Configure firewall policy offload level.	option	-	disable
	Option	Description		
	disable	Disable policy offloading.		
	dos-offload	Only enable DoS policy offloading.		
prp-trailer-action	Enable/disable action to take on PRP trailer.	option	-	disable
	Option	Description		
	enable	Try to keep PRP trailer.		
	disable	Trim PRP trailer.		
sccp-port	TCP port the SCCP proxy monitors for SCCP traffic (0 - 65535, default = 2000).	integer	Minimum value: 0 Maximum value: 65535	2000
sctp-session-without-init	Enable/disable Sctp session creation without Sctp INIT.	option	-	disable
	Option	Description		
	enable	Enable Sctp session creation without Sctp INIT.		
	disable	Disable Sctp session creation without Sctp INIT.		
ses-denied-multicast-traffic	Enable/disable including denied multicast session in the session table.	option	-	disable
	Option	Description		
	enable	Include denied multicast sessions in the session table.		
	disable	Do not add denied multicast sessions to the session table.		
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-	disable
	Option	Description		
	enable	Include denied sessions in the session table.		
	disable	Do not add denied sessions to the session table.		
sip-expectation	Enable/disable the SIP kernel session helper to create an expectation for port 5060.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Allow SIP session helper to create an expectation for port 5060.		
	<i>disable</i>	Prevent SIP session helper from creating an expectation for port 5060.		
sip-nat-trace	Enable/disable recording the original SIP source IP address when NAT is used.	option	-	enable
	Option Description			
	<i>enable</i>	Record the original SIP source IP address when NAT is used.		
	<i>disable</i>	Do not record the original SIP source IP address when NAT is used.		
sip-ssl-port	TCP port the SIP proxy monitors for SIP SSL/TLS traffic (0 - 65535, default = 5061).	integer	Minimum value: 5061 0 Maximum value: 65535	
sip-tcp-port	TCP port the SIP proxy monitors for SIP traffic (0 - 65535, default = 5060).	integer	Minimum value: 5060 1 Maximum value: 65535	
sip-udp-port	UDP port the SIP proxy monitors for SIP traffic (0 - 65535, default = 5060).	integer	Minimum value: 5060 1 Maximum value: 65535	
snat-hairpin-traffic	Enable/disable source NAT (SNAT) for VIP hairpin traffic.	option	-	enable
	Option Description			
	<i>enable</i>	Enable SNAT for VIP hairpin traffic.		
	<i>disable</i>	Disable SNAT for VIP hairpin traffic.		
status	Enable/disable this VDOM.	option	-	enable
	Option Description			
	<i>enable</i>	Enable this VDOM.		
	<i>disable</i>	Disable this VDOM.		
strict-src-check	Enable/disable strict source verification.	option	-	disable
	Option Description			
	<i>enable</i>	Enable strict source verification.		
	<i>disable</i>	Disable strict source verification.		

Parameter	Description	Type	Size	Default										
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow TCP session without SYN flags.</td></tr><tr><td><i>disable</i></td><td>Do not allow TCP session without SYN flags.</td></tr></table>	Option	Description	<i>enable</i>	Allow TCP session without SYN flags.	<i>disable</i>	Do not allow TCP session without SYN flags.							
Option	Description													
<i>enable</i>	Allow TCP session without SYN flags.													
<i>disable</i>	Do not allow TCP session without SYN flags.													
utf8-spam-tagging	Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Convert antispam tags to UTF-8.</td></tr><tr><td><i>disable</i></td><td>Do not convert antispam tags.</td></tr></table>	Option	Description	<i>enable</i>	Convert antispam tags to UTF-8.	<i>disable</i>	Do not convert antispam tags.							
Option	Description													
<i>enable</i>	Convert antispam tags to UTF-8.													
<i>disable</i>	Do not convert antispam tags.													
v4-ecmp-mode	IPv4 Equal-cost multi-path (ECMP) routing and load balancing mode.	option	-	source-ip-based										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>source-ip-based</i></td><td>Select next hop based on source IP.</td></tr><tr><td><i>weight-based</i></td><td>Select next hop based on weight.</td></tr><tr><td><i>usage-based</i></td><td>Select next hop based on usage.</td></tr><tr><td><i>source-dest-ip-based</i></td><td>Select next hop based on both source and destination IPs.</td></tr></table>	Option	Description	<i>source-ip-based</i>	Select next hop based on source IP.	<i>weight-based</i>	Select next hop based on weight.	<i>usage-based</i>	Select next hop based on usage.	<i>source-dest-ip-based</i>	Select next hop based on both source and destination IPs.			
Option	Description													
<i>source-ip-based</i>	Select next hop based on source IP.													
<i>weight-based</i>	Select next hop based on weight.													
<i>usage-based</i>	Select next hop based on usage.													
<i>source-dest-ip-based</i>	Select next hop based on both source and destination IPs.													
vdom-type	Vdom type (traffic, lan-extension or admin).	option	-	traffic										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>traffic</i></td><td>Change to traffic VDOM</td></tr><tr><td><i>lan-extension</i></td><td>Change to lan-extension VDOM</td></tr><tr><td><i>admin</i></td><td>Change to admin VDOM</td></tr></table>	Option	Description	<i>traffic</i>	Change to traffic VDOM	<i>lan-extension</i>	Change to lan-extension VDOM	<i>admin</i>	Change to admin VDOM					
Option	Description													
<i>traffic</i>	Change to traffic VDOM													
<i>lan-extension</i>	Change to lan-extension VDOM													
<i>admin</i>	Change to admin VDOM													
vpn-stats-log	Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a space.	option	-	ipsec pptp l2tp ssl **										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipsec</i></td><td>IPsec.</td></tr></table>	Option	Description	<i>ipsec</i>	IPsec.									
Option	Description													
<i>ipsec</i>	IPsec.													

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pptp</i>	PPTP.		
	<i>l2tp</i>	L2TP.		
	<i>ssl</i>	SSL.		
vpn-stats-period	Period to send VPN log statistics (0 or 60 - 86400 sec).	integer	Minimum value: 600 0 Maximum value: 4294967295	600
wccp-cache-engine	Enable/disable WCCP cache engine.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WCCP cache engine.		
	<i>disable</i>	Disable WCCP cache engine.		

* This parameter may not exist in some models.

** Values may differ between models.

config system sflow

Configure sFlow.

```

config system sflow
  Description: Configure sFlow.
  config collectors
    Description: sFlow collectors.
    edit <id>
      set collector-ip {ipv4-address}
      set collector-port {integer}
      set interface {string}
      set interface-select-method [auto|sdwan|...]
      set source-ip {ipv4-address}
    next
  end
end
end

```

config collectors

Parameter	Description	Type	Size	Default								
collector-ip	IP addresses of the sFlow collectors that sFlow agents added to interfaces in this VDOM send sFlow datagrams to.	ipv4-address	Not Specified	0.0.0.0								
collector-port	UDP port number used for sending sFlow datagrams (configure only if required by your sFlow collector or your network configuration) (0 - 65535, default = 6343).	integer	Minimum value: 0 Maximum value: 65535	6343								
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified	0.0.0.0								

config system sit-tunnel

Configure IPv6 tunnel over IPv4.

```
config system sit-tunnel
  Description: Configure IPv6 tunnel over IPv4.
  edit <name>
    set auto-asic-offload [enable|disable]
    set destination {ipv4-address}
    set interface {string}
    set ip6 {ipv6-prefix}
    set source {ipv4-address}
    set use-sdwan [disable|enable]
  next
end
```

config system sit-tunnel

Parameter	Description	Type	Size	Default						
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable auto ASIC offloading.</td></tr><tr><td>disable</td><td>Disable ASIC offloading.</td></tr></table>	Option	Description	enable	Enable auto ASIC offloading.	disable	Disable ASIC offloading.			
Option	Description									
enable	Enable auto ASIC offloading.									
disable	Disable ASIC offloading.									
destination	Destination IP address of the tunnel.	ipv4-address	Not Specified	0.0.0.0						
interface	Interface name.	string	Maximum length: 15							
ip6	IPv6 address of the tunnel.	ipv6-prefix	Not Specified	::/0						
name	Tunnel name.	string	Maximum length: 15							
source	Source IP address of the tunnel.	ipv4-address	Not Specified	0.0.0.0						
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of SD-WAN to reach remote gateway.</td></tr><tr><td>enable</td><td>Enable use of SD-WAN to reach remote gateway.</td></tr></table>	Option	Description	disable	Disable use of SD-WAN to reach remote gateway.	enable	Enable use of SD-WAN to reach remote gateway.			
Option	Description									
disable	Disable use of SD-WAN to reach remote gateway.									
enable	Enable use of SD-WAN to reach remote gateway.									

* This parameter may not exist in some models.

config system smc-ntp



This command is available for model(s): FortiGate 1100E, FortiGate 1101E, FortiGate 1800F, FortiGate 1801F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700F, FortiGate 3701F, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 900G, FortiGate 901G.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 120G, FortiGate 121G, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3700D, FortiGate 3960E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure SMC NTP information.

```
config system smc-ntp
  Description: Configure SMC NTP information.
  set channel {integer}
  config ntpserver
    Description: Configure the FortiGate SMC to connect to an NTP server.
    edit <id>
      set server {ipv4-address}
    next
  end
  set ntpsync [enable|disable]
  set syncinterval {integer}
end
```

config system smc-ntp

Parameter	Description	Type	Size	Default
channel	SMC NTP client will send NTP packets through this channel.	integer	Minimum value: 1 Maximum value: 65535	5
ntpsync	Enable/disable setting the FortiGate SMC system time by synchronizing with an NTP server.	option	-	disable
	Option	Description		
	enable	Enable synchronization with NTP server in SMC.		
	disable	Disable synchronization with NTP server in SMC.		
syncinterval	SMC NTP synchronization interval (1 - 65535 secs).	integer	Minimum value: 1 Maximum value: 65535	60

config ntpserver

Parameter	Description	Type	Size	Default
id	NTP server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server	IP address of the NTP server.	ipv4-address	Not Specified	0.0.0.0

config system sms-server

Configure SMS server for sending SMS messages to support user authentication.

```
config system sms-server
  Description: Configure SMS server for sending SMS messages to support user authentication.
  edit <name>
    set mail-server {string}
  next
end
```

config system sms-server

Parameter	Description	Type	Size	Default
mail-server	Email-to-SMS server domain name.	string	Maximum length: 63	
name	Name of SMS server.	string	Maximum length: 35	

config system snmp community

SNMP community configuration.

```
config system snmp community
  Description: SNMP community configuration.
  edit <id>
    set events {option1}, {option2}, ...
    config hosts
      Description: Configure IPv4 SNMP managers (hosts).
      edit <id>
        set ha-direct [enable|disable]
        set host-type [any|query|...]
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set ip {user}
        set source-ip {ipv4-address}
        set vrf-select {integer}
      next
    end
    config hosts6
      Description: Configure IPv6 SNMP managers.
      edit <id>
        set ha-direct [enable|disable]
        set host-type [any|query|...]
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set ipv6 {ipv6-prefix}
        set source-ipv6 {ipv6-address}
        set vrf-select {integer}
      next
    end
    set mib-view {string}
    set name {string}
    set query-v1-port {integer}
    set query-v1-status [enable|disable]
    set query-v2c-port {integer}
    set query-v2c-status [enable|disable]
    set status [enable|disable]
    set trap-v1-lport {integer}
```

```
    set trap-v1-rport {integer}
    set trap-v1-status [enable|disable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set trap-v2c-status [enable|disable]
    set vdoms <name1>, <name2>, ...
next
end
```

config system snmp community

Parameter	Description	Type	Size	Default
events	SNMP trap events.	option	-	cpu-high mem- low log-full intf-ip vpn-tun- up vpn-tun- down ha- switch ha-hb- failure ips- signature ips- anomaly av- virus av- oversize av- pattern av- fragmented fm- if-change bgp- established bgp-backward- transition ha- member-up ha- member-down ent-conf- change av- conserve av- bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open temperature- high voltage- alert power- supply faz- disconnect faz fan-failure wc- ap-up wc-ap- down fswctl- session-up fswctl-session- down load- balance-real- server-down per-cpu-high dhcp pool- usage ippool interface ospf- nbr-state- change ospf- virtnbr-state- change **

Parameter	Description	Type	Size	Default

Option	Description
<i>cpu-high</i>	Send a trap when CPU usage is high.
<i>mem-low</i>	Send a trap when used memory is high, free memory is low, or freeable memory is high.
<i>log-full</i>	Send a trap when log disk space becomes low.
<i>intf-ip</i>	Send a trap when an interface IP address is changed.
<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.
<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.
<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.
<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.
<i>ips-signature</i>	Send a trap when IPS detects an attack.
<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.
<i>av-virus</i>	Send a trap when AntiVirus finds a virus.
<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.
<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.
<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.
<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.
<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.
<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.
<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.
<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.
<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).
<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.
<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.		
	<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.		
	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.		
	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.		
	<i>temperature-high</i>	Send a trap when a temperature sensor registers a temperature that is too high.		
	<i>voltage-alert</i>	Send a trap when a voltage sensor registers a voltage that is outside of the normal range.		
	<i>power-supply</i>	Send a trap when a power supply fails or restores.		
	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.		
	<i>faz</i>	Send a trap when Fortianalyzer main server failover and alternate server take over, or alternate server failover and main server take over.		
	<i>fan-failure</i>	Send a trap when a fan fails.		
	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.		
	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.		
	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.		
	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.		
	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.		
	<i>device-new</i>	Send a trap when a new device is found.		
	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.		
	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.		
	<i>pool-usage</i>	Send a trap about ippool usage.		
	<i>ippool</i>	Send a trap for ippool events.		
	<i>interface</i>	Send a trap for interface event.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ospf-nbr-state-change</i>	Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.		
	<i>ospf-virtnbr-state-change</i>	Send a trap when there has been a change in the state of an OSPF virtual neighbor.		
id	Community ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
mib-view	SNMP access control MIB view.	string	Maximum length: 32	
name	Community name.	string	Maximum length: 35	
query-v1-port	SNMP v1 query port (default = 161).	integer	Minimum value: 1 1 Maximum value: 65535	161
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
query-v2c-port	SNMP v2c query port (default = 161).	integer	Minimum value: 161 0 Maximum value: 65535	
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
status	Enable/disable this SNMP community.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
trap-v1-lport	SNMP v1 trap local port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v1-rport	SNMP v1 trap remote port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-v2c-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v2c-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
vdoms <name>	SNMP access control VDOMs. VDOM name.	string	Maximum length: 79							

** Values may differ between models.

config hosts

Parameter	Description	Type	Size	Default						
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default								
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both. No traps will be sent when IP type is subnet.	option	-	any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept queries from and send traps to this SNMP manager.</td></tr><tr><td><i>query</i></td><td>Accept queries from this SNMP manager but do not send traps.</td></tr><tr><td><i>trap</i></td><td>Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.</td></tr></table>	Option	Description	<i>any</i>	Accept queries from and send traps to this SNMP manager.	<i>query</i>	Accept queries from this SNMP manager but do not send traps.	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.			
Option	Description											
<i>any</i>	Accept queries from and send traps to this SNMP manager.											
<i>query</i>	Accept queries from this SNMP manager but do not send traps.											
<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.											
id	Host entry ID.	integer	Minimum value: 0 0 Maximum value: 4294967295									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
ip	IPv4 address of the SNMP manager (host).	user	Not Specified									
source-ip	Source IPv4 address for SNMP traps.	ipv4-address	Not Specified	0.0.0.0								
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 0 Maximum value: 511									

config hosts6

Parameter	Description	Type	Size	Default
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-	any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept queries from and send traps to this SNMP manager.</td></tr><tr><td><i>query</i></td><td>Accept queries from this SNMP manager but do not send traps.</td></tr><tr><td><i>trap</i></td><td>Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.</td></tr></table>	Option	Description	<i>any</i>	Accept queries from and send traps to this SNMP manager.	<i>query</i>	Accept queries from this SNMP manager but do not send traps.	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.			
	Option	Description										
	<i>any</i>	Accept queries from and send traps to this SNMP manager.										
	<i>query</i>	Accept queries from this SNMP manager but do not send traps.										
<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.											
id	Host6 entry ID.	integer	Minimum value: 0 Maximum value: 4294967295									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
ipv6	SNMP manager IPv6 address prefix.	ipv6-prefix	Not Specified	::/0								
source-ipv6	Source IPv6 address for SNMP traps.	ipv6-address	Not Specified	::								
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511									

config system snmp mib-view

SNMP Access Control MIB View configuration.

```

config system snmp mib-view
    Description: SNMP Access Control MIB View configuration.
    edit <name>
        set exclude {string}
        set include {string}
    next
end

```

config system snmp mib-view

Parameter	Description	Type	Size	Default
exclude	OID subtrees to be excluded in the view. Maximum 64 allowed.	string	Maximum length: 79	
include	OID subtrees to be included in the view. Maximum 16 allowed.	string	Maximum length: 79	
name	MIB view name.	string	Maximum length: 32	

config system snmp rmon-stat

SNMP Remote Network Monitoring (RMON) Ethernet statistics configuration.

```

config system snmp rmon-stat
    Description: SNMP Remote Network Monitoring (RMON) Ethernet statistics configuration.
    edit <id>
        set owner {string}
        set source {string}
    next
end

```

config system snmp rmon-stat

Parameter	Description	Type	Size	Default
id	RMON Ethernet statistics entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	
owner	Owner of the Ethernet statistics entry.	string	Maximum length: 127	
source	Data source of the Ethernet statistics entry.	string	Maximum length: 15	

config system snmp sysinfo

SNMP system info configuration.

```
config system snmp sysinfo
  Description: SNMP system info configuration.
  set append-index [enable|disable]
  set contact-info {var-string}
  set description {var-string}
  set engine-id {string}
  set engine-id-type [text|hex|...]
  set location {var-string}
  set non-mgmt-vdom-query [enable|disable]
  set status [enable|disable]
  set trap-free-memory-threshold {integer}
  set trap-freeable-memory-threshold {integer}
  set trap-high-cpu-threshold {integer}
  set trap-log-full-threshold {integer}
  set trap-low-memory-threshold {integer}
end
```

config system snmp sysinfo

Parameter	Description	Type	Size	Default
append-index	Enable/disable allowance of appending vdom or interface index in some RFC tables.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
contact-info	Contact information.	var-string	Maximum length: 255	
description	System description.	var-string	Maximum length: 255	
engine-id	Local SNMP engineID string (maximum 27 characters).	string	Maximum length: 54	
engine-id-type	Local SNMP engineID type (text/hex/mac).	option	-	text
	Option		Description	
	<i>text</i>		Text format.	

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hex</td><td>Octets format.</td></tr><tr><td>mac</td><td>MAC address format.</td></tr></table>	Option	Description	hex	Octets format.	mac	MAC address format.			
	Option	Description								
	hex	Octets format.								
mac	MAC address format.									
location	System location.	var-string	Maximum length: 255							
non-mgmt-vdom-query	Enable/disable allowance of SNMPv3 query from non-management vdoms.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									
status	Enable/disable SNMP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									
trap-free-memory-threshold	Free memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	5						
trap-freeable-memory-threshold	Freeable memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	60						
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80						
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	90						
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80						

config system snmp user

SNMP user configuration.

```
config system snmp user
  Description: SNMP user configuration.
  edit <name>
    set auth-proto [md5|sha|...]
    set auth-pwd {password}
    set events {option1}, {option2}, ...
    set ha-direct [enable|disable]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set mib-view {string}
    set notify-hosts {ipv4-address}
    set notify-hosts6 {ipv6-address}
    set priv-proto [aes|des|...]
    set priv-pwd {password}
    set queries [enable|disable]
    set query-port {integer}
    set security-level [no-auth-no-priv|auth-no-priv|...]
    set source-ip {ipv4-address}
    set source-ipv6 {ipv6-address}
    set status [enable|disable]
    set trap-lport {integer}
    set trap-rport {integer}
    set trap-status [enable|disable]
    set vdoms <name1>, <name2>, ...
    set vrf-select {integer}
  next
end
```

config system snmp user

Parameter	Description	Type	Size	Default														
auth-proto	Authentication protocol.	option	-	sha														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>md5</td><td>HMAC-MD5-96 authentication protocol.</td></tr><tr><td>sha</td><td>HMAC-SHA-96 authentication protocol.</td></tr><tr><td>sha224</td><td>HMAC-SHA224 authentication protocol.</td></tr><tr><td>sha256</td><td>HMAC-SHA256 authentication protocol.</td></tr><tr><td>sha384</td><td>HMAC-SHA384 authentication protocol.</td></tr><tr><td>sha512</td><td>HMAC-SHA512 authentication protocol.</td></tr></table>				Option	Description	md5	HMAC-MD5-96 authentication protocol.	sha	HMAC-SHA-96 authentication protocol.	sha224	HMAC-SHA224 authentication protocol.	sha256	HMAC-SHA256 authentication protocol.	sha384	HMAC-SHA384 authentication protocol.	sha512	HMAC-SHA512 authentication protocol.
	Option	Description																
	md5	HMAC-MD5-96 authentication protocol.																
	sha	HMAC-SHA-96 authentication protocol.																
	sha224	HMAC-SHA224 authentication protocol.																
	sha256	HMAC-SHA256 authentication protocol.																
	sha384	HMAC-SHA384 authentication protocol.																
sha512	HMAC-SHA512 authentication protocol.																	

Parameter	Description	Type	Size	Default
auth-pwd	Password for authentication protocol.	password	Not Specified	

Parameter	Description	Type	Size	Default
events	SNMP notifications (traps) to send.	option	-	cpu-high mem- low log-full intf-ip vpn-tun- up vpn-tun- down ha- switch ha-hb- failure ips- signature ips- anomaly av- virus av- oversize av- pattern av- fragmented fm- if-change bgp- established bgp-backward- transition ha- member-up ha- member-down ent-conf- change av- conserve av- bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open temperature- high voltage- alert power- supply faz- disconnect faz fan-failure wc- ap-up wc-ap- down fswctl- session-up fswctl-session- down load- balance-real- server-down per-cpu-high dhcp pool- usage ippool interface ospf- nbr-state- change ospf- virtnbr-state- change **

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>cpu-high</i>	Send a trap when CPU usage is high.		
	<i>mem-low</i>	Send a trap when used memory is high, free memory is low, or freeable memory is high.		
	<i>log-full</i>	Send a trap when log disk space becomes low.		
	<i>intf-ip</i>	Send a trap when an interface IP address is changed.		
	<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.		
	<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.		
	<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.		
	<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.		
	<i>ips-signature</i>	Send a trap when IPS detects an attack.		
	<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.		
	<i>av-virus</i>	Send a trap when AntiVirus finds a virus.		
	<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.		
	<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.		
	<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.		
	<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.		
	<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.		
	<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.		
	<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.		
	<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.		
	<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.		
	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).		
	<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.		
	<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.		
	<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.		
	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.		
	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.		
	<i>temperature-high</i>	Send a trap when a temperature sensor registers a temperature that is too high.		
	<i>voltage-alert</i>	Send a trap when a voltage sensor registers a voltage that is outside of the normal range.		
	<i>power-supply</i>	Send a trap when a power supply fails or restores.		
	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.		
	<i>faz</i>	Send a trap when Fortianalyzer main server failover and alternate server take over, or alternate server failover and main server take over.		
	<i>fan-failure</i>	Send a trap when a fan fails.		
	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.		
	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.		
	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.		
	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.		
	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.		
	<i>device-new</i>	Send a trap when a new device is found.		
	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.		
	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.		
	<i>pool-usage</i>	Send a trap about ippool usage.		
	<i>ippool</i>	Send a trap for ippool events.		
	<i>interface</i>	Send a trap for interface event.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ospf-nbr-state-change</i></td><td>Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.</td></tr><tr><td><i>ospf-virtnbr-state-change</i></td><td>Send a trap when there has been a change in the state of an OSPF virtual neighbor.</td></tr></table>	Option	Description	<i>ospf-nbr-state-change</i>	Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.	<i>ospf-virtnbr-state-change</i>	Send a trap when there has been a change in the state of an OSPF virtual neighbor.					
	Option	Description										
	<i>ospf-nbr-state-change</i>	Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.										
<i>ospf-virtnbr-state-change</i>	Send a trap when there has been a change in the state of an OSPF virtual neighbor.											
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
mib-view	SNMP access control MIB view.	string	Maximum length: 32									
name	SNMP user name.	string	Maximum length: 32									
notify-hosts	SNMP managers to send notifications (traps) to.	ipv4-address	Not Specified									
notify-hosts6	IPv6 SNMP managers to send notifications (traps) to.	ipv6-address	Not Specified									
priv-proto	Privacy (encryption) protocol.	option	-	aes								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aes</i></td><td>CFB128-AES-128 symmetric encryption protocol.</td></tr><tr><td><i>des</i></td><td>CBC-DES symmetric encryption protocol.</td></tr><tr><td><i>aes256</i></td><td>CFB128-AES-256 symmetric encryption protocol.</td></tr></table>	Option	Description	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.	<i>des</i>	CBC-DES symmetric encryption protocol.	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.			
	Option	Description										
	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.										
	<i>des</i>	CBC-DES symmetric encryption protocol.										
<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.											

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aes256cisco</i></td><td>CFB128-AES-256 symmetric encryption protocol compatible with CISCO.</td></tr></table>	Option	Description	<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.							
Option	Description											
<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.											
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified									
queries	Enable/disable SNMP queries for this user.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
query-port	SNMPv3 query port (default = 161).	integer	Minimum value: 1 Maximum value: 65535	161								
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-auth-no-priv</i></td><td>Message with no authentication and no privacy (encryption).</td></tr><tr><td><i>auth-no-priv</i></td><td>Message with authentication but no privacy (encryption).</td></tr><tr><td><i>auth-priv</i></td><td>Message with authentication and privacy (encryption).</td></tr></table>	Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).			
Option	Description											
<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).											
<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).											
<i>auth-priv</i>	Message with authentication and privacy (encryption).											
source-ip	Source IP for SNMP trap.	ipv4-address	Not Specified	0.0.0.0								
source-ipv6	Source IPv6 for SNMP trap.	ipv6-address	Not Specified	::								
status	Enable/disable this SNMP user.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
trap-lport	SNMPv3 local trap port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162								

Parameter	Description	Type	Size	Default
trap-rport	SNMPv3 trap remote port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162
trap-status	Enable/disable traps for this SNMP user.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
vdoms <name>	SNMP access control VDOMs. VDOM name.	string	Maximum length: 79	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

** Values may differ between models.

config system speed-test-schedule

Speed test schedule for each interface.

```

config system speed-test-schedule
  Description: Speed test schedule for each interface.
  edit <interface>
    set ctrl-port {integer}
    set diffserv {user}
    set dynamic-server [disable|enable]
    set mode [UDP|TCP|...]
    set schedules <name1>, <name2>, ...
    set server-name {string}
    set server-port {integer}
    set status [disable|enable]
    set update-inbandwidth [disable|enable]
    set update-inbandwidth-maximum {integer}
    set update-inbandwidth-minimum {integer}
    set update-outbandwidth [disable|enable]
    set update-outbandwidth-maximum {integer}
    set update-outbandwidth-minimum {integer}
    set update-shaper [disable|local|...]
  next
end

```

config system speed-test-schedule

Parameter	Description	Type	Size	Default								
ctrl-port	Port of the controller to get access token.	integer	Minimum value: 1 Maximum value: 65535	5200								
diffserv	DSCP used for speed test.	user	Not Specified									
dynamic-server	Enable/disable dynamic server option.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable dynamic server.</td></tr><tr><td>enable</td><td>Enable dynamic server.The speed test server will be found automatically.</td></tr></table>	Option	Description	disable	Disable dynamic server.	enable	Enable dynamic server.The speed test server will be found automatically.					
Option	Description											
disable	Disable dynamic server.											
enable	Enable dynamic server.The speed test server will be found automatically.											
interface	Interface name.	string	Maximum length: 35									
mode	Protocol Auto(default), TCP or UDP used for speed test.	option	-	Auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>UDP</td><td>Protocol UDP for speed test.</td></tr><tr><td>TCP</td><td>Protocol TCP for speed test.</td></tr><tr><td>Auto</td><td>Dynamically selects TCP or UDP based on the speed test setting</td></tr></table>	Option	Description	UDP	Protocol UDP for speed test.	TCP	Protocol TCP for speed test.	Auto	Dynamically selects TCP or UDP based on the speed test setting			
Option	Description											
UDP	Protocol UDP for speed test.											
TCP	Protocol TCP for speed test.											
Auto	Dynamically selects TCP or UDP based on the speed test setting											
schedules <name>	Schedules for the interface. Name of a firewall recurring schedule.	string	Maximum length: 31									
server-name	Speed test server name.	string	Maximum length: 35									
server-port	Port of the server to run speed test.	integer	Minimum value: 1 Maximum value: 65535	5201								
status	Enable/disable scheduled speed test.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable scheduled speed test.</td></tr><tr><td>enable</td><td>Enable scheduled speed test.</td></tr></table>	Option	Description	disable	Disable scheduled speed test.	enable	Enable scheduled speed test.					
Option	Description											
disable	Disable scheduled speed test.											
enable	Enable scheduled speed test.											

Parameter	Description	Type	Size	Default										
update-inbandwidth	Enable/disable bypassing interface's inbound bandwidth setting.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Honor interface's inbandwidth shaping.</td></tr><tr><td>enable</td><td>Ignore interface's inbandwidth shaping.</td></tr></table>	Option	Description	disable	Honor interface's inbandwidth shaping.	enable	Ignore interface's inbandwidth shaping.							
	Option	Description												
	disable	Honor interface's inbandwidth shaping.												
enable	Ignore interface's inbandwidth shaping.													
update-inbandwidth-maximum	Maximum downloading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0										
update-inbandwidth-minimum	Minimum downloading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0										
update-outbandwidth	Enable/disable bypassing interface's outbound bandwidth setting.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Honor interface's outbandwidth shaping.</td></tr><tr><td>enable</td><td>Ignore updating interface's outbandwidth shaping.</td></tr></table>	Option	Description	disable	Honor interface's outbandwidth shaping.	enable	Ignore updating interface's outbandwidth shaping.							
	Option	Description												
	disable	Honor interface's outbandwidth shaping.												
enable	Ignore updating interface's outbandwidth shaping.													
update-outbandwidth-maximum	Maximum uploading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0										
update-outbandwidth-minimum	Minimum uploading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0										
update-shaper	Set egress shaper based on the test result.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable updating egress shaper.</td></tr><tr><td>local</td><td>Update local-side egress shaper.</td></tr><tr><td>remote</td><td>Update remote-side egress shaper.</td></tr><tr><td>both</td><td>Update both local-side and remote-side egress shaper.</td></tr></table>	Option	Description	disable	Disable updating egress shaper.	local	Update local-side egress shaper.	remote	Update remote-side egress shaper.	both	Update both local-side and remote-side egress shaper.			
	Option	Description												
	disable	Disable updating egress shaper.												
	local	Update local-side egress shaper.												
	remote	Update remote-side egress shaper.												
both	Update both local-side and remote-side egress shaper.													

config system speed-test-server



The `config system speed-test-server` command is read-only. Administrators cannot configure custom servers.

Configure speed test server list.

```
config system speed-test-server
  Description: Configure speed test server list.
  edit <name>
    config host
      Description: Hosts of the server.
      edit <id>
        set distance {integer}
        set ip {ipv4-address}
        set latitude {string}
        set longitude {string}
        set password {password}
        set port {integer}
        set user {string}
      next
    end
    set timestamp {integer}
  next
end
```

config system speed-test-server

Parameter	Description	Type	Size	Default
name	Speed test server name.	string	Maximum length: 35	
timestamp	Speed test server timestamp.	integer	Minimum value: 0 Maximum value: 4294967295	

config host

Parameter	Description	Type	Size	Default
distance	Speed test host distance.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
id	Server host ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
ip	Server host IPv4 address.	ipv4-address	Not Specified	0.0.0.0
latitude	Speed test host latitude.	string	Maximum length: 7	
longitude	Speed test host longitude.	string	Maximum length: 7	
password	Speed test host password.	password	Not Specified	
port	Server host port number to communicate with client.	integer	Minimum value: 5204 1 Maximum value: 65535	
user	Speed test host user name.	string	Maximum length: 64	

config system speed-test-setting

Configure speed test setting.

```
config system speed-test-setting
    Description: Configure speed test setting.
    set latency-threshold {integer}
    set multiple-tcp-stream {integer}
end
```

config system speed-test-setting

Parameter	Description	Type	Size	Default
latency-threshold	Speed test latency threshold in milliseconds (0 - 2000, default = 60) for the Auto mode. If the latency exceeds this threshold, the speed test will use the UDP protocol; otherwise, it will use the TCP protocol.	integer	Minimum value: 0 Maximum value: 2000	60
multiple-tcp-stream	Number of parallel client streams (1 - 64, default = 4) for the TCP protocol to run during the speed test.	integer	Minimum value: 1 Maximum value: 64	4

config system ssh-config

Configure SSH config.

```
config system ssh-config
  Description: Configure SSH config.
  set ssh-enc-algo {option1}, {option2}, ...
  set ssh-hsk {user}
  set ssh-hsk-algo {option1}, {option2}, ...
  set ssh-hsk-override [disable|enable]
  set ssh-hsk-password {password}
  set ssh-kex-algo {option1}, {option2}, ...
  set ssh-mac-algo {option1}, {option2}, ...
end
```

config system ssh-config

Parameter	Description	Type	Size	Default
ssh-enc-algo	Select one or more SSH ciphers.	option	-	aes256-ctr aes256-gcm@openssh.com
		Option	Description	
		<i>chacha20-poly1305@openssh.com</i>	chacha20-poly1305@openssh.com	
		<i>aes128-ctr</i>	aes128-ctr	
		<i>aes192-ctr</i>	aes192-ctr	
		<i>aes256-ctr</i>	aes256-ctr	
		<i>arcfour256</i>	arcfour256	
		<i>arcfour128</i>	arcfour128	
		<i>aes128-cbc</i>	aes128-cbc	
		<i>3des-cbc</i>	3des-cbc	
		<i>blowfish-cbc</i>	blowfish-cbc	
		<i>cast128-cbc</i>	cast128-cbc	
		<i>aes192-cbc</i>	aes192-cbc	
		<i>aes256-cbc</i>	aes256-cbc	
		<i>arcfour</i>	arcfour	
		<i>rijndael-cbc@lysator.liu.se</i>	rijndael-cbc@lysator.liu.se	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>aes128-gcm@openssh.com</i>	aes128-gcm@openssh.com		
	<i>aes256-gcm@openssh.com</i>	aes256-gcm@openssh.com		
ssh-hsk	Config SSH host key.	user	Not Specified	
ssh-hsk-algo	Select one or more SSH hostkey algorithms.	option	-	ecdsa-sha2-nistp521 ecdsa-sha2-nistp384 ecdsa-sha2-nistp256 rsa-sha2-256 rsa-sha2-512 ssh-ed25519
	Option	Description		
	<i>ssh-rsa</i>	ssh-rsa		
	<i>ecdsa-sha2-nistp521</i>	ecdsa-sha2-nistp521		
	<i>ecdsa-sha2-nistp384</i>	ecdsa-sha2-nistp384		
	<i>ecdsa-sha2-nistp256</i>	ecdsa-sha2-nistp256		
	<i>rsa-sha2-256</i>	rsa-sha2-256		
	<i>rsa-sha2-512</i>	rsa-sha2-512		
<i>ssh-ed25519</i>	ssh-ed25519			
ssh-hsk-override	Enable/disable SSH host key override in SSH daemon.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SSH host key override in SSH daemon.		
	<i>enable</i>	Enable SSH host key override in SSH daemon.		
ssh-hsk-password	Password for ssh-hostkey.	password	Not Specified	

Parameter	Description	Type	Size	Default
ssh-kex-algo	Select one or more SSH kex algorithms.	option	-	diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
Option		Description		
<i>diffie-hellman-group1-sha1</i>		diffie-hellman-group1-sha1		
<i>diffie-hellman-group14-sha1</i>		diffie-hellman-group14-sha1		
<i>diffie-hellman-group14-sha256</i>		diffie-hellman-group14-sha256		
<i>diffie-hellman-group16-sha512</i>		diffie-hellman-group16-sha512		
<i>diffie-hellman-group18-sha512</i>		diffie-hellman-group18-sha512		
<i>diffie-hellman-group-exchange-sha1</i>		diffie-hellman-group-exchange-sha1		
<i>diffie-hellman-group-exchange-sha256</i>		diffie-hellman-group-exchange-sha256		
<i>curve25519-sha256@libssh.org</i>		curve25519-sha256@libssh.org		
<i>ecdh-sha2-nistp256</i>		ecdh-sha2-nistp256		
<i>ecdh-sha2-nistp384</i>		ecdh-sha2-nistp384		
<i>ecdh-sha2-nistp521</i>		ecdh-sha2-nistp521		

Parameter	Description	Type	Size	Default
ssh-mac-algo	Select one or more SSH MAC algorithms.	option	-	hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512 hmac-sha2-512-etm@openssh.com
Option		Description		
<i>hmac-md5</i>		hmac-md5		
<i>hmac-md5-etm@openssh.com</i>		hmac-md5-etm@openssh.com		
<i>hmac-md5-96</i>		hmac-md5-96		
<i>hmac-md5-96-etm@openssh.com</i>		hmac-md5-96-etm@openssh.com		
<i>hmac-sha1</i>		hmac-sha1		
<i>hmac-sha1-etm@openssh.com</i>		hmac-sha1-etm@openssh.com		
<i>hmac-sha2-256</i>		hmac-sha2-256		
<i>hmac-sha2-256-etm@openssh.com</i>		hmac-sha2-256-etm@openssh.com		
<i>hmac-sha2-512</i>		hmac-sha2-512		
<i>hmac-sha2-512-etm@openssh.com</i>		hmac-sha2-512-etm@openssh.com		
<i>hmac-ripemd160</i>		hmac-ripemd160		
<i>hmac-ripemd160@openssh.com</i>		hmac-ripemd160@openssh.com		
<i>hmac-ripemd160-etm@openssh.com</i>		hmac-ripemd160-etm@openssh.com		
<i>umac-64@openssh.com</i>		umac-64@openssh.com		
<i>umac-128@openssh.com</i>		umac-128@openssh.com		
<i>umac-64-etm@openssh.com</i>		umac-64-etm@openssh.com		
<i>umac-128-etm@openssh.com</i>		umac-128-etm@openssh.com		

config system sso-admin

Configure SSO admin users.

```
config system sso-admin
  Description: Configure SSO admin users.
  edit <name>
    set accprofile {string}
    set vdom <name1>, <name2>, ...
  next
end
```

config system sso-admin

Parameter	Description	Type	Size	Default
accprofile	SSO admin user access profile.	string	Maximum length: 35	
name	SSO admin name.	string	Maximum length: 64	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system sso-forticloud-admin

Configure FortiCloud SSO admin users.

```
config system sso-forticloud-admin
  Description: Configure FortiCloud SSO admin users.
  edit <name>
    set accprofile {string}
    set vdom <name1>, <name2>, ...
  next
end
```

config system sso-forticloud-admin

Parameter	Description	Type	Size	Default
accprofile	FortiCloud SSO admin user access profile.	string	Maximum length: 35	
name	FortiCloud SSO admin name.	string	Maximum length: 64	

Parameter	Description	Type	Size	Default
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system sso-fortigate-cloud-admin

Configure FortiCloud SSO admin users.

```
config system sso-fortigate-cloud-admin
  Description: Configure FortiCloud SSO admin users.
  edit <name>
    set accprofile {string}
    set vdom <name1>, <name2>, ...
  next
end
```

config system sso-fortigate-cloud-admin

Parameter	Description	Type	Size	Default
accprofile	FortiCloud SSO admin user access profile.	string	Maximum length: 35	
name	FortiCloud SSO admin name.	string	Maximum length: 64	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system standalone-cluster

Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.

```
config system standalone-cluster
  Description: Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.
  set asymmetric-traffic-control [cps-preferred|strict-anti-replay]
  config cluster-peer
    Description: Configure FortiGate Session Life Support Protocol (FGSP) session
    synchronization.
    edit <sync-id>
      set down-intfs-before-sess-sync <name1>, <name2>, ...
      set hb-interval {integer}
      set hb-lost-threshold {integer}
      set ipsec-tunnel-sync [enable|disable]
      set peerip {ipv4-address}
```

```

    set peervd {string}
    set secondary-add-ipsec-routes [enable|disable]
    config session-sync-filter
        Description: Add one or more filters if you only want to synchronize some
sessions. Use the filter to configure the types of sessions to synchronize.
        config custom-service
            Description: Only sessions using these custom services are synchronized. Use
source and destination port ranges to define these custom services.
            edit <id>
                set dst-port-range {user}
                set src-port-range {user}
            next
        end
        set dstaddr {ipv4-classnet-any}
        set dstaddr6 {ipv6-network}
        set dstintf {string}
        set srcaddr {ipv4-classnet-any}
        set srcaddr6 {ipv6-network}
        set srcintf {string}
    end
    set syncvd <name1>, <name2>, ...
next
end
set encryption [enable|disable]
set group-member-id {integer}
set layer2-connection [available|unavailable]
set monitor-interface <name1>, <name2>, ...
config monitor-prefix
    Description: Configure a list of routing prefixes to monitor.
    edit <id>
        set prefix {ipv4-classnet-any}
        set vdom {string}
        set vrf {integer}
    next
end
set pingsvr-monitor-interface <name1>, <name2>, ...
set psksecret {password-3}
set session-sync-dev {user}
set standalone-group-id {integer}
end

```

config system standalone-cluster

Parameter	Description	Type	Size	Default
asymmetric-traffic-control	Asymmetric traffic control mode.	option	-	cps-preferred

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cps-preferred</i></td><td>Connection per second (CPS) preferred.</td></tr><tr><td><i>strict-anti-replay</i></td><td>Strict anti-replay check.</td></tr></table>	Option	Description	<i>cps-preferred</i>	Connection per second (CPS) preferred.	<i>strict-anti-replay</i>	Strict anti-replay check.			
	Option	Description								
	<i>cps-preferred</i>	Connection per second (CPS) preferred.								
<i>strict-anti-replay</i>	Strict anti-replay check.									
encryption	Enable/disable encryption when synchronizing sessions.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable encryption when synchronizing sessions.</td></tr><tr><td><i>disable</i></td><td>Disable encryption when synchronizing sessions.</td></tr></table>	Option	Description	<i>enable</i>	Enable encryption when synchronizing sessions.	<i>disable</i>	Disable encryption when synchronizing sessions.			
	Option	Description								
	<i>enable</i>	Enable encryption when synchronizing sessions.								
<i>disable</i>	Disable encryption when synchronizing sessions.									
group-member-id	Cluster member ID (0 - 15).	integer	Minimum value: 0 Maximum value: 15	0						
layer2-connection	Indicate whether layer 2 connections are present among FGSP members.	option	-	unavailable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>available</i></td><td>There exist layer 2 connections among FGSP members.</td></tr><tr><td><i>unavailable</i></td><td>There does not exist layer 2 connection among FGSP members.</td></tr></table>	Option	Description	<i>available</i>	There exist layer 2 connections among FGSP members.	<i>unavailable</i>	There does not exist layer 2 connection among FGSP members.			
	Option	Description								
	<i>available</i>	There exist layer 2 connections among FGSP members.								
<i>unavailable</i>	There does not exist layer 2 connection among FGSP members.									
monitor-interface <name>	Configure a list of interfaces on which to monitor itself. Monitoring is performed on the status of the interface. Interface name.	string	Maximum length: 79							
pingsvr-monitor-interface <name>	List of pingsvr monitor interface to check for remote IP monitoring. Interface name.	string	Maximum length: 79							
psksecret	Pre-shared secret for session synchronization (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified							
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified							
standalone-group-id	Cluster group ID (0 - 255). Must be the same for all members.	integer	Minimum value: 0 Maximum value: 255	0						

config cluster-peer

Parameter	Description	Type	Size	Default						
down-intfs-before-sess-sync <name>	List of interfaces to be turned down before session synchronization is complete. Interface name.	string	Maximum length: 79							
hb-interval	Heartbeat interval (1 - 20 (100*ms). Increase to reduce false positives.	integer	Minimum value: 2 1 Maximum value: 20							
hb-lost-threshold	Lost heartbeat threshold (1 - 60). Increase to reduce false positives.	integer	Minimum value: 10 1 Maximum value: 60							
ipsec-tunnel-sync	Enable/disable IPsec tunnel synchronization.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec tunnel synchronization.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec tunnel synchronization.</td></tr></table>				Option	Description	<i>enable</i>	Enable IPsec tunnel synchronization.	<i>disable</i>	Disable IPsec tunnel synchronization.
Option	Description									
<i>enable</i>	Enable IPsec tunnel synchronization.									
<i>disable</i>	Disable IPsec tunnel synchronization.									
peerip	IP address of the interface on the peer unit that is used for the session synchronization link.	ipv4-address	Not Specified	0.0.0.0						
peervd	VDOM that contains the session synchronization link interface on the peer unit. Usually both peers would have the same peervd.	string	Maximum length: 31	root						
secondary-add-ipsec-routes	Enable/disable IKE route announcement on the backup unit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Add IKE routes to the backup unit.</td></tr><tr><td><i>disable</i></td><td>Do not add IKE routes to the backup unit.</td></tr></table>				Option	Description	<i>enable</i>	Add IKE routes to the backup unit.	<i>disable</i>	Do not add IKE routes to the backup unit.
Option	Description									
<i>enable</i>	Add IKE routes to the backup unit.									
<i>disable</i>	Do not add IKE routes to the backup unit.									
sync-id	Sync ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
syncvd <name>	Sessions from these VDOMs are synchronized using this session synchronization configuration. VDOM name.	string	Maximum length: 79							

config session-sync-filter

Parameter	Description	Type	Size	Default
dstaddr	Only sessions to this IPv4 address are synchronized.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dstaddr6	Only sessions to this IPv6 address are synchronized.	ipv6-network	Not Specified	::/0
dstintf	Only sessions to this interface are synchronized.	string	Maximum length: 15	
srcaddr	Only sessions from this IPv4 address are synchronized.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
srcaddr6	Only sessions from this IPv6 address are synchronized.	ipv6-network	Not Specified	::/0
srcintf	Only sessions from this interface are synchronized.	string	Maximum length: 15	

config custom-service

Parameter	Description	Type	Size	Default
dst-port-range	Custom service destination port range.	user	Not Specified	0-0
id	Custom service ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
src-port-range	Custom service source port range.	user	Not Specified	0-0

config monitor-prefix

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
prefix	Prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
vdom	VDOM name.	string	Maximum length: 31	
vrf	VRF ID.	integer	Minimum value: 0 Maximum value: 511	

config system storage

Configure logical storage.

```

config system storage
  Description: Configure logical storage.
  edit <name>
    set device {string}
    set media-status [enable|disable|...]
    set order {integer}
    set partition {string}
    set size {integer}
    set status [enable|disable]
    set usage [log|wanopt]
    set wanopt-mode [mix|wanopt|...]
  next
end

```

config system storage

Parameter	Description	Type	Size	Default								
device	Partition device.	string	Maximum length: 19	?								
media-status	The physical status of current media.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Storage is enabled.</td></tr><tr><td><i>disable</i></td><td>Storage is disabled.</td></tr><tr><td><i>fail</i></td><td>Storage have some fail sector.</td></tr></table>				Option	Description	<i>enable</i>	Storage is enabled.	<i>disable</i>	Storage is disabled.	<i>fail</i>	Storage have some fail sector.
	Option	Description										
	<i>enable</i>	Storage is enabled.										
	<i>disable</i>	Storage is disabled.										
<i>fail</i>	Storage have some fail sector.											
name	Storage name.	string	Maximum length: 35	default_n								
order	Set storage order.	integer	Minimum value: 0 0 Maximum value: 255									

Parameter	Description	Type	Size	Default
partition	Label of underlying partition.	string	Maximum length: 16	<unknown>
size	Partition size.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
status	Enable/disable storage.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
usage *	Use hard disk for logging or WAN Optimization (default = log).	option	-	log **
	Option	Description		
	log	Use hard disk for logging.		
	wanopt	Use hard disk for WAN Optimization.		
wanopt-mode *	WAN Optimization mode (default = mix).	option	-	mix
	Option	Description		
	mix	Use hard disk for WAN Optimization mix mode.		
	wanopt	Use hard disk for WAN Optimization wanopt mode.		
	webcache	Use hard disk for WAN Optimization webcache mode.		

* This parameter may not exist in some models.

** Values may differ between models.

config system stp



This command is available for model(s): FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 200F, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3200F, FortiGate 3201F, FortiGate 3500F, FortiGate 3501F, FortiGate 3700F, FortiGate 3701F, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

Configure Spanning Tree Protocol (STP).

```
config system stp
  Description: Configure Spanning Tree Protocol (STP).
  set forward-delay {integer}
  set hello-time {integer}
  set max-age {integer}
  set max-hops {integer}
  set switch-priority [0|4096|...]
end
```

config system stp

Parameter	Description	Type	Size	Default
forward-delay	Forward delay (4 - 30 sec, default = 15).	integer	Minimum value: 4 Maximum value: 30	15

Parameter	Description	Type	Size	Default																																
hello-time	Hello time (1 - 10 sec, default = 2).	integer	Minimum value: 1 Maximum value: 10	2																																
max-age	Maximum packet age (6 - 40 sec, default = 20).	integer	Minimum value: 6 Maximum value: 40	20																																
max-hops	Maximum number of hops (1 - 40, default = 20).	integer	Minimum value: 1 Maximum value: 40	20																																
switch-priority	STP switch priority; the lower the number the higher the priority (select from 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, and 57344).	option	-	32768																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>0</td></tr><tr><td>4096</td><td>4096</td></tr><tr><td>8192</td><td>8192</td></tr><tr><td>12288</td><td>12288</td></tr><tr><td>16384</td><td>16384</td></tr><tr><td>20480</td><td>20480</td></tr><tr><td>24576</td><td>24576</td></tr><tr><td>28672</td><td>28672</td></tr><tr><td>32768</td><td>32768</td></tr><tr><td>36864</td><td>36864</td></tr><tr><td>40960</td><td>40960</td></tr><tr><td>45056</td><td>45056</td></tr><tr><td>49152</td><td>49152</td></tr><tr><td>53248</td><td>53248</td></tr><tr><td>57344</td><td>57344</td></tr></table>				Option	Description	0	0	4096	4096	8192	8192	12288	12288	16384	16384	20480	20480	24576	24576	28672	28672	32768	32768	36864	36864	40960	40960	45056	45056	49152	49152	53248	53248	57344	57344
Option	Description																																			
0	0																																			
4096	4096																																			
8192	8192																																			
12288	12288																																			
16384	16384																																			
20480	20480																																			
24576	24576																																			
28672	28672																																			
32768	32768																																			
36864	36864																																			
40960	40960																																			
45056	45056																																			
49152	49152																																			
53248	53248																																			
57344	57344																																			

config system switch-interface

Configure software switch interfaces by grouping physical and WiFi interfaces.

```

config system switch-interface
    Description: Configure software switch interfaces by grouping physical and WiFi interfaces.
    edit <name>
        set intra-switch-policy [implicit|explicit]
        set mac-ttl {integer}
        set member <interface-name1>, <interface-name2>, ...
        set span [disable|enable]
        set span-dest-port {string}
        set span-direction [rx|tx|...]
        set span-source-port <interface-name1>, <interface-name2>, ...
        set type [switch|hub]
        set vdom {string}
    next
end

```

config system switch-interface

Parameter	Description	Type	Size	Default						
intra-switch-policy	Allow any traffic between switch interfaces or require firewall policies to allow traffic between switch interfaces.	option	-	implicit						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>implicit</i></td><td>Traffic between switch members is implicitly allowed.</td></tr><tr><td><i>explicit</i></td><td>Traffic between switch members must match firewall policies.</td></tr></table>	Option	Description	<i>implicit</i>	Traffic between switch members is implicitly allowed.	<i>explicit</i>	Traffic between switch members must match firewall policies.			
Option	Description									
<i>implicit</i>	Traffic between switch members is implicitly allowed.									
<i>explicit</i>	Traffic between switch members must match firewall policies.									
mac-ttl	Duration for which MAC addresses are held in the ARP table (300 - 8640000 sec, default = 300).	integer	Minimum value: 300 Maximum value: 8640000	300						
member <interface-name>	Names of the interfaces that belong to the virtual switch. Interface name.	string	Maximum length: 79							
name	Interface name (name cannot be in use by any other interfaces, VLANs, or inter-VDOM links).	string	Maximum length: 15							
span	Enable/disable port spanning. Port spanning echoes traffic received by the software switch to the span destination port.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable port spanning.</td></tr><tr><td><i>enable</i></td><td>Enable port spanning.</td></tr></table>	Option	Description	<i>disable</i>	Disable port spanning.	<i>enable</i>	Enable port spanning.			
Option	Description									
<i>disable</i>	Disable port spanning.									
<i>enable</i>	Enable port spanning.									

Parameter	Description	Type	Size	Default								
span-dest-port	SPAN destination port name. All traffic on the SPAN source ports is echoed to the SPAN destination port.	string	Maximum length: 15									
span-direction	The direction in which the SPAN port operates, either: rx, tx, or both.	option	-	both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>rx</td><td>Copies only received packets from source SPAN ports to the destination SPAN port.</td></tr><tr><td>tx</td><td>Copies only transmitted packets from source SPAN ports to the destination SPAN port.</td></tr><tr><td>both</td><td>Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.</td></tr></table>	Option	Description	rx	Copies only received packets from source SPAN ports to the destination SPAN port.	tx	Copies only transmitted packets from source SPAN ports to the destination SPAN port.	both	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.			
Option	Description											
rx	Copies only received packets from source SPAN ports to the destination SPAN port.											
tx	Copies only transmitted packets from source SPAN ports to the destination SPAN port.											
both	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.											
span-source-port <interface-name>	Physical interface name. Port spanning echoes all traffic on the SPAN source ports to the SPAN destination port. Physical interface name.	string	Maximum length: 79									
type	Type of switch based on functionality: switch for normal functionality, or hub to duplicate packets to all port members.	option	-	switch								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>switch</td><td>Switch for normal switch functionality (available in NAT mode only).</td></tr><tr><td>hub</td><td>Hub to duplicate packets to all member ports.</td></tr></table>	Option	Description	switch	Switch for normal switch functionality (available in NAT mode only).	hub	Hub to duplicate packets to all member ports.					
Option	Description											
switch	Switch for normal switch functionality (available in NAT mode only).											
hub	Hub to duplicate packets to all member ports.											
vdom	VDOM that the software switch belongs to.	string	Maximum length: 31									

config system timezone

Show timezone. Read-only.

```

config system timezone
  Description: Show timezone. Read-only.
  edit <name>
  next
end

```

config system timezone

Parameter	Description	Type	Size	Default
name	Database name of a timezone.	string	Maximum length: 63	

config system tos-based-priority

Configure Type of Service (ToS) based priority table to set network traffic priorities.

```
config system tos-based-priority
  Description: Configure Type of Service (ToS) based priority table to set network traffic
  priorities.
  edit <id>
    set priority [low|medium|...]
    set tos {integer}
  next
end
```

config system tos-based-priority

Parameter	Description	Type	Size	Default
id	Item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
priority	ToS based priority level to low, medium or high (these priorities match firewall traffic shaping priorities) (default = medium).	option	-	high
	Option	Description		
	<i>low</i>	Low priority.		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		
tos	Value of the ToS byte in the IP datagram header (0-15, 8: minimize delay, 4: maximize throughput, 2: maximize reliability, 1: minimize monetary cost, and 0: default service).	integer	Minimum value: 0 Maximum value: 15	0

config system vdom

Configure virtual domain.

```
config system vdom
  Description: Configure virtual domain.
  edit <name>
    set flag {integer}
    set short-name {string}
    set vcluster-id {integer}
  next
end
```

config system vdom

Parameter	Description	Type	Size	Default
flag	Flag.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	VDOM name.	string	Maximum length: 31	
short-name	VDOM short name.	string	Maximum length: 11	
vcluster-id	Virtual cluster ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0

config system vdom-dns

Configure DNS servers for a non-management VDOM.

```
config system vdom-dns
  Description: Configure DNS servers for a non-management VDOM.
  set alt-primary {ipv4-address}
  set alt-secondary {ipv4-address}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ip6-primary {ipv6-address}
  set ip6-secondary {ipv6-address}
  set primary {ipv4-address}
  set protocol {option1}, {option2}, ...
  set secondary {ipv4-address}
```

```

set server-hostname <hostname1>, <hostname2>, ...
set server-select-method [least-rtt|failover]
set source-ip {ipv4-address}
set source-ip-interface {string}
set ssl-certificate {string}
set vdom-dns [enable|disable]
set vrf-select {integer}
end

```

config system vdom-dns

Parameter	Description	Type	Size	Default								
alt-primary	Alternate primary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0								
alt-secondary	Alternate secondary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
ip6-primary	Primary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::								
ip6-secondary	Secondary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::								
primary	Primary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0								
protocol	DNS transport protocols.	option	-	cleartext								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cleartext</i></td><td>DNS over UDP/53, DNS over TCP/53.</td></tr><tr><td><i>dot</i></td><td>DNS over TLS/853.</td></tr><tr><td><i>doh</i></td><td>DNS over HTTPS/443.</td></tr></table>				Option	Description	<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.	<i>dot</i>	DNS over TLS/853.	<i>doh</i>	DNS over HTTPS/443.
Option	Description											
<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.											
<i>dot</i>	DNS over TLS/853.											
<i>doh</i>	DNS over HTTPS/443.											

Parameter	Description	Type	Size	Default						
secondary	Secondary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0						
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127							
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>least-rtt</i></td><td>Select servers based on least round trip time.</td></tr><tr><td><i>failover</i></td><td>Select servers based on the order they are configured.</td></tr></table>				Option	Description	<i>least-rtt</i>	Select servers based on least round trip time.	<i>failover</i>	Select servers based on the order they are configured.
Option	Description									
<i>least-rtt</i>	Select servers based on least round trip time.									
<i>failover</i>	Select servers based on the order they are configured.									
source-ip	Source IP for communications with the DNS server.	ipv4-address	Not Specified	0.0.0.0						
source-ip-interface	IP address of the specified interface as the source IP address.	string	Maximum length: 15							
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory						
vdom-dns	Enable/disable configuring DNS servers for the current VDOM.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable configuring DNS servers for the current VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable configuring DNS servers for the current VDOM.</td></tr></table>				Option	Description	<i>enable</i>	Enable configuring DNS servers for the current VDOM.	<i>disable</i>	Disable configuring DNS servers for the current VDOM.
Option	Description									
<i>enable</i>	Enable configuring DNS servers for the current VDOM.									
<i>disable</i>	Disable configuring DNS servers for the current VDOM.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config system vdom-exception

Global configuration objects that can be configured independently across different ha peers for all VDOMs or for the defined VDOM scope.

```
config system vdom-exception
  Description: Global configuration objects that can be configured independently across
  different ha peers for all VDOMs or for the defined VDOM scope.
  edit <id>
    set object [log.fortianalyzer.setting|log.fortianalyzer.override-setting|...]
    set scope [all|inclusive|...]
```

```

        set vdom <name1>, <name2>, ...
    next
end

```

config system vdom-exception

Parameter	Description	Type	Size	Default
id	Index (1 - 4096).	integer	Minimum value: 1 Maximum value: 4096	0
object	Name of the configuration object that can be configured independently for all VDOMs.	option	-	

Option	Description
<i>log.fortianalyzer.setting</i>	log.fortianalyzer.setting
<i>log.fortianalyzer.override-setting</i>	log.fortianalyzer.override-setting
<i>log.fortianalyzer2.setting</i>	log.fortianalyzer2.setting
<i>log.fortianalyzer2.override-setting</i>	log.fortianalyzer2.override-setting
<i>log.fortianalyzer3.setting</i>	log.fortianalyzer3.setting
<i>log.fortianalyzer3.override-setting</i>	log.fortianalyzer3.override-setting
<i>log.fortianalyzer-cloud.setting</i>	log.fortianalyzer-cloud.setting
<i>log.fortianalyzer-cloud.override-setting</i>	log.fortianalyzer-cloud.override-setting
<i>log.syslogd.setting</i>	log.syslogd.setting
<i>log.syslogd.override-setting</i>	log.syslogd.override-setting
<i>log.syslogd2.setting</i>	log.syslogd2.setting
<i>log.syslogd2.override-setting</i>	log.syslogd2.override-setting
<i>log.syslogd3.setting</i>	log.syslogd3.setting
<i>log.syslogd3.override-setting</i>	log.syslogd3.override-setting
<i>log.syslogd4.setting</i>	log.syslogd4.setting
<i>log.syslogd4.override-setting</i>	log.syslogd4.override-setting

Parameter	Description	Type	Size	Default																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>system.gre-tunnel</i></td><td>system.gre-tunnel</td></tr><tr><td><i>system.central-management</i></td><td>system.central-management</td></tr><tr><td><i>system.csf</i></td><td>system.csf</td></tr><tr><td><i>user.radius</i></td><td>user.radius</td></tr><tr><td><i>system.interface</i></td><td>system.interface</td></tr><tr><td><i>log.syslogd.setting</i></td><td>log.syslogd.setting</td></tr><tr><td><i>log.syslogd.override-setting</i></td><td>log.syslogd.override-setting</td></tr><tr><td><i>firewall.address</i></td><td>firewall.address</td></tr></table>		Option	Description	<i>system.gre-tunnel</i>	system.gre-tunnel	<i>system.central-management</i>	system.central-management	<i>system.csf</i>	system.csf	<i>user.radius</i>	user.radius	<i>system.interface</i>	system.interface	<i>log.syslogd.setting</i>	log.syslogd.setting	<i>log.syslogd.override-setting</i>	log.syslogd.override-setting	<i>firewall.address</i>	firewall.address			
	Option	Description																					
	<i>system.gre-tunnel</i>	system.gre-tunnel																					
	<i>system.central-management</i>	system.central-management																					
	<i>system.csf</i>	system.csf																					
	<i>user.radius</i>	user.radius																					
	<i>system.interface</i>	system.interface																					
	<i>log.syslogd.setting</i>	log.syslogd.setting																					
	<i>log.syslogd.override-setting</i>	log.syslogd.override-setting																					
<i>firewall.address</i>	firewall.address																						
scope	Determine whether the configuration object can be configured separately for all VDOMs or if some VDOMs share the same configuration.	option	-	all																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Object configuration independent for all VDOMs.</td></tr><tr><td><i>inclusive</i></td><td>Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.</td></tr><tr><td><i>exclusive</i></td><td>Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.</td></tr></table>		Option	Description	<i>all</i>	Object configuration independent for all VDOMs.	<i>inclusive</i>	Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.	<i>exclusive</i>	Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.													
	Option	Description																					
	<i>all</i>	Object configuration independent for all VDOMs.																					
	<i>inclusive</i>	Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.																					
<i>exclusive</i>	Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.																						
vdom <name>	Names of the VDOMs. VDOM name.	string	Maximum length: 79																				

config system vdom-link

Configure VDOM links.

```

config system vdom-link
  Description: Configure VDOM links.
  edit <name>
    set type [ppp|ethernet]
    set vcluster [vcluster1|vcluster2]
  next
end

```

config system vdom-link

Parameter	Description	Type	Size	Default
name	VDOM link name (maximum = 11 characters).	string	Maximum length: 11	
type	VDOM link type: PPP or Ethernet.	option	-	ppp
	Option	Description		
	<i>ppp</i>	PPP VDOM link.		
	<i>ethernet</i>	Ethernet VDOM link.		
vcluster	Virtual cluster.	option	-	vcluster1
	Option	Description		
	<i>vcluster1</i>	Virtual cluster 1.		
	<i>vcluster2</i>	Virtual cluster 2.		

config system vdom-netflow

Configure NetFlow per VDOM.

```
config system vdom-netflow
  Description: Configure NetFlow per VDOM.
  config collectors
    Description: Netflow collectors.
    edit <id>
      set collector-ip {string}
      set collector-port {integer}
      set interface {string}
      set interface-select-method [auto|sdwan|...]
      set source-ip {string}
      set source-ip-interface {string}
      set vrf-select {integer}
    next
  end
  set vdom-netflow [enable|disable]
end
```

config system vdom-netflow

Parameter	Description	Type	Size	Default
vdom-netflow	Enable/disable NetFlow per VDOM.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable NetFlow per VDOM.		
	<i>disable</i>	Disable NetFlow per VDOM.		

config collectors

Parameter	Description	Type	Size	Default
collector-ip	Collector IP.	string	Maximum length: 63	
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535	2055
id	ID.	integer	Minimum value: 1 Maximum value: 6	0
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
source-ip	Source IP address for communication with the NetFlow agent.	string	Maximum length: 63	
source-ip-interface	Name of the interface used to determine the source IP for exporting packets.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config system vdom-property

Configure VDOM property.

```

config system vdom-property
  Description: Configure VDOM property.
  edit <name>
    set custom-service {user}
    set description {string}
    set dialup-tunnel {user}
    set firewall-address {user}
    set firewall-addrgroup {user}
    set firewall-policy {user}
    set ipsec-phase1 {user}
    set ipsec-phase1-interface {user}
    set ipsec-phase2 {user}
    set ipsec-phase2-interface {user}
    set log-disk-quota {user}
    set onetime-schedule {user}
    set proxy {user}
    set recurring-schedule {user}
    set service-group {user}
    set session {user}
    set snmp-index {integer}
    set sslvpn {user}
    set user {user}
    set user-group {user}
  next
end

```

config system vdom-property

Parameter	Description	Type	Size	Default
custom-service	Maximum guaranteed number of firewall custom services.	user	Not Specified	
description	Description.	string	Maximum length: 127	
dialup-tunnel	Maximum guaranteed number of dial-up tunnels.	user	Not Specified	

Parameter	Description	Type	Size	Default
firewall-address	Maximum guaranteed number of firewall addresses (IPv4, IPv6, multicast).	user	Not Specified	
firewall-addrgrp	Maximum guaranteed number of firewall address groups (IPv4, IPv6).	user	Not Specified	
firewall-policy	Maximum guaranteed number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	user	Not Specified	
ipsec-phase1	Maximum guaranteed number of VPN IPsec phase 1 tunnels.	user	Not Specified	
ipsec-phase1-interface	Maximum guaranteed number of VPN IPsec phase1 interface tunnels.	user	Not Specified	
ipsec-phase2	Maximum guaranteed number of VPN IPsec phase 2 tunnels.	user	Not Specified	
ipsec-phase2-interface	Maximum guaranteed number of VPN IPsec phase2 interface tunnels.	user	Not Specified	
log-disk-quota	Log disk quota in megabytes (MB). Range depends on how much disk space is available.	user	Not Specified	
name	VDOM name.	string	Maximum length: 31	
onetime-schedule	Maximum guaranteed number of firewall one-time schedules.	user	Not Specified	
proxy *	Maximum guaranteed number of concurrent proxy users.	user	Not Specified	
recurring-schedule	Maximum guaranteed number of firewall recurring schedules.	user	Not Specified	
service-group	Maximum guaranteed number of firewall service groups.	user	Not Specified	
session	Maximum guaranteed number of sessions.	user	Not Specified	
snmp-index	Permanent SNMP Index of the virtual domain (1 - 2147483647).	integer	Minimum value: 1 Maximum value: 2147483647	0
sslvpn *	Maximum guaranteed number of Agentless VPNs.	user	Not Specified	
user	Maximum guaranteed number of local users.	user	Not Specified	
user-group	Maximum guaranteed number of user groups.	user	Not Specified	

* This parameter may not exist in some models.

config system vdom-radius-server

Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM.

```
config system vdom-radius-server
    Description: Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for
this VDOM.
    edit <name>
        set radius-server-vdom {string}
        set status [enable|disable]
    next
end
```

config system vdom-radius-server

Parameter	Description	Type	Size	Default
name	Name of the VDOM that you are adding the RADIUS server to.	string	Maximum length: 31	
radius-server-vdom	Use this option to select another VDOM containing a VDOM RSSO RADIUS server to use for the current VDOM.	string	Maximum length: 31	
status	Enable/disable the RSSO RADIUS server for this VDOM.	option	-	disable
		Option	Description	
		enable	Enable the RSSO RADIUS server for this VDOM.	
		disable	Disable the RSSO RADIUS server for this VDOM.	

config system vdom-sflow

Configure sFlow per VDOM to add or change the IP address and UDP port that FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.

```
config system vdom-sflow
    Description: Configure sFlow per VDOM to add or change the IP address and UDP port that
FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.
    config collectors
        Description: sFlow collectors.
        edit <id>
            set collector-ip {ipv4-address}
            set collector-port {integer}
            set interface {string}
            set interface-select-method [auto|sdwan|...]
        next
    end
```

```

        set source-ip {ipv4-address}
    next
end
set vdom-sflow [enable|disable]
end

```

config system vdom-sflow

Parameter	Description	Type	Size	Default						
vdom-sflow	Enable/disable the sFlow configuration for the current VDOM.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sFlow for this VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable sFlow for this VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable sFlow for this VDOM.	<i>disable</i>	Disable sFlow for this VDOM.			
Option	Description									
<i>enable</i>	Enable sFlow for this VDOM.									
<i>disable</i>	Disable sFlow for this VDOM.									

config collectors

Parameter	Description	Type	Size	Default								
collector-ip	IP addresses of the sFlow collectors that sFlow agents added to interfaces in this VDOM send sFlow datagrams to.	ipv4-address	Not Specified	0.0.0.0								
collector-port	UDP port number used for sending sFlow datagrams (configure only if required by your sFlow collector or your network configuration) (0 - 65535, default = 6343).	integer	Minimum value: 0 Maximum value: 65535	6343								
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											

Parameter	Description	Type	Size	Default
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified	0.0.0.0

config system vin-alarm



This command is available for model(s): FortiGateRugged 70F 3G4G, FortiGateRugged 70F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure vin alarm settings.

```
config system vin-alarm
  Description: Configure vin alarm settings.
  set psu-1-initial-voltage {integer}
  set psu-1-threshold-low-percent {integer}
  set psu-2-initial-voltage {integer}
  set psu-2-threshold-low-percent {integer}
  set status [disable|enable]
end
```


config system vin-alarm

Parameter	Description	Type	Size	Default
psu-1-initial-voltage	Initial voltage for the first PSU	integer	Minimum value: 10 Maximum value: 125	0
psu-1-threshold-low-percent	Percentage threshold at which the first PSU voltage drops to trigger a low voltage alarm (default = 80)	integer	Minimum value: 1 Maximum value: 99	80
psu-2-initial-voltage	Initial voltage for the second PSU	integer	Minimum value: 10 Maximum value: 125	0
psu-2-threshold-low-percent	Percentage threshold at which the second PSU voltage drops to trigger a low voltage alarm (default = 80)	integer	Minimum value: 1 Maximum value: 99	80
status	Enable/disable vin alarm.	option	-	disable
		Option	Description	
		<i>disable</i>	Disable vin alarm.	
		<i>enable</i>	Enable vin alarm.	

config system virtual-switch



This command is available for model(s): FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 200F, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3200F, FortiGate 3201F, FortiGate 3500F, FortiGate 3501F, FortiGate 3700F, FortiGate 3701F, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64.

Configure virtual hardware switch interfaces.

```
config system virtual-switch
  Description: Configure virtual hardware switch interfaces.
  edit <name>
    set physical-switch {string}
    config port
      Description: Configure member ports.
      edit <name>
        set alias {string}
      next
    end
    set span [disable|enable]
    set span-dest-port {string}
    set span-direction [rx|tx|...]
    set span-source-port {string}
    set vlan {integer}
  next
end
```

config system virtual-switch

Parameter	Description	Type	Size	Default								
name	Name of the virtual switch.	string	Maximum length: 15									
physical-switch	Physical switch parent.	string	Maximum length: 15									
span *	Enable/disable SPAN.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SPAN.</td></tr><tr><td><i>enable</i></td><td>Enable SPAN.</td></tr></table>	Option	Description	<i>disable</i>	Disable SPAN.	<i>enable</i>	Enable SPAN.					
Option	Description											
<i>disable</i>	Disable SPAN.											
<i>enable</i>	Enable SPAN.											
span-dest-port *	SPAN destination port.	string	Maximum length: 15									
span-direction *	SPAN direction.	option	-	both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rx</i></td><td>SPAN receive direction only.</td></tr><tr><td><i>tx</i></td><td>SPAN transmit direction only.</td></tr><tr><td><i>both</i></td><td>SPAN both directions.</td></tr></table>	Option	Description	<i>rx</i>	SPAN receive direction only.	<i>tx</i>	SPAN transmit direction only.	<i>both</i>	SPAN both directions.			
Option	Description											
<i>rx</i>	SPAN receive direction only.											
<i>tx</i>	SPAN transmit direction only.											
<i>both</i>	SPAN both directions.											
span-source-port *	SPAN source port.	string	Maximum length: 15									
vlan *	VLAN.	integer	Minimum value: 0 Maximum value: 4294967295									

* This parameter may not exist in some models.

config port

Parameter	Description	Type	Size	Default
alias	Alias.	string	Maximum length: 25	
name	Physical interface name.	string	Maximum length: 15	

config system virtual-wire-pair

Configure virtual wire pairs.

```
config system virtual-wire-pair
  Description: Configure virtual wire pairs.
  edit <name>
    set member <interface-name1>, <interface-name2>, ...
    set outer-vlan-id <vlanid1>, <vlanid2>, ...
    set poweroff-bypass [enable|disable]
    set poweron-bypass [enable|disable]
    set vlan-filter {user}
    set wildcard-vlan [enable|disable]
  next
end
```

config system virtual-wire-pair

Parameter	Description	Type	Size	Default						
member <interface-name>	Interfaces belong to the virtual-wire-pair. Interface name.	string	Maximum length: 79							
name	Virtual-wire-pair name. Must be a unique interface name.	string	Maximum length: 11							
outer-vlan-id <vlanid> *	Outer VLAN ID. VLAN ID (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094							
poweroff-bypass *	Enable/disable interface bypass state when power off.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable bypass when power off.</td></tr><tr><td>disable</td><td>Disable bypass when power off.</td></tr></table>	Option	Description	enable	Enable bypass when power off.	disable	Disable bypass when power off.			
Option	Description									
enable	Enable bypass when power off.									
disable	Disable bypass when power off.									
poweron-bypass *	Enable/disable interface bypass state when power on.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable bypass when power on.</td></tr><tr><td>disable</td><td>Disable bypass when power on.</td></tr></table>	Option	Description	enable	Enable bypass when power on.	disable	Disable bypass when power on.			
Option	Description									
enable	Enable bypass when power on.									
disable	Disable bypass when power on.									

Parameter	Description	Type	Size	Default
vlan-filter	VLAN ranges to allow	user	Not Specified	
wildcard-vlan	Enable/disable wildcard VLAN.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable wildcard VLAN.		
	<i>disable</i>	Disable wildcard VLAN.		

* This parameter may not exist in some models.

config system vene-interface

Configure virtual network enabler tunnels.

```

config system vene-interface
    Description: Configure virtual network enabler tunnels.
    edit <name>
        set auto-asic-offload [enable|disable]
        set bmr-hostname {password}
        set br {string}
        set http-password {password}
        set http-username {string}
        set interface {string}
        set ipv4-address {ipv4-classnet-host}
        set mode [map-e|fixed-ip|...]
        set ssl-certificate {string}
        set update-url {string}
    next
end

```

config system vene-interface

Parameter	Description	Type	Size	Default
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable auto ASIC offloading.		
	<i>disable</i>	Disable ASIC offloading.		

Parameter	Description	Type	Size	Default								
bmr-hostname	BMR hostname.	password	Not Specified									
br	IPv6 address or FQDN of the border relay.	string	Maximum length: 255									
http-password	HTTP authentication password.	password	Not Specified									
http-username	HTTP authentication user name.	string	Maximum length: 64									
interface	Interface name.	string	Maximum length: 15									
ipv4-address	Tunnel IPv4 address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								
mode	VNE tunnel mode.	option	-	map-e								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>map-e</td><td>Map-e mode.</td></tr><tr><td>fixed-ip</td><td>Fixed-ip mode.</td></tr><tr><td>ds-lite</td><td>DS-Lite mode.</td></tr></table>				Option	Description	map-e	Map-e mode.	fixed-ip	Fixed-ip mode.	ds-lite	DS-Lite mode.
Option	Description											
map-e	Map-e mode.											
fixed-ip	Fixed-ip mode.											
ds-lite	DS-Lite mode.											
name	VNE tunnel name.	string	Maximum length: 15									
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory								
update-url	URL of provisioning server.	string	Maximum length: 511									

* This parameter may not exist in some models.

config system vpce



This command is available for model(s): FortiGate-VM64 Aliyun, FortiGate-VM64 GCP. It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure system VPC configuration.

```
config system vpce
  Description: Configure system VPC configuration.
  edit <id>
    set endpoint-id {string}
    set name {string}
    set vdom {string}
  next
end
```

config system vpce

Parameter	Description	Type	Size	Default
endpoint-id	VPC endpoint ID.	string	Maximum length: 32	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
name	VPC endpoint name.	string	Maximum length: 63	
vdom	VDOM name.	string	Maximum length: 31	

config system vxlan

Configure VXLAN devices.

```

config system vxlan
  Description: Configure VXLAN devices.
  edit <name>
    set dstport {integer}
    set evpn-id {integer}
    set interface {string}
    set ip-version [ipv4-unicast|ipv6-unicast|...]
    set learn-from-traffic [enable|disable]
    set multicast-ttl {integer}
    set remote-ip <ip1>, <ip2>, ...
    set remote-ip6 <ip61>, <ip62>, ...
    set vni {integer}
  next
end

```

config system vxlan

Parameter	Description	Type	Size	Default
dstport	VXLAN destination port (1 - 65535, default = 4789).	integer	Minimum value: 1 Maximum value: 65535	4789
evpn-id	EVPN instance.	integer	Minimum value: 1 Maximum value: 65535	0
interface	Outgoing interface for VXLAN encapsulated traffic.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default										
ip-version	IP version to use for the VXLAN interface and so for communication over the VXLAN. IPv4 or IPv6 unicast or multicast.	option	-	ipv4-unicast										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4-unicast</td><td>Use IPv4 unicast addressing over the VXLAN.</td></tr><tr><td>ipv6-unicast</td><td>Use IPv6 unicast addressing over the VXLAN.</td></tr><tr><td>ipv4-multicast</td><td>Use IPv4 multicast addressing over the VXLAN.</td></tr><tr><td>ipv6-multicast</td><td>Use IPv6 multicast addressing over the VXLAN.</td></tr></table>	Option	Description	ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.	ipv6-unicast	Use IPv6 unicast addressing over the VXLAN.	ipv4-multicast	Use IPv4 multicast addressing over the VXLAN.	ipv6-multicast	Use IPv6 multicast addressing over the VXLAN.			
Option	Description													
ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.													
ipv6-unicast	Use IPv6 unicast addressing over the VXLAN.													
ipv4-multicast	Use IPv4 multicast addressing over the VXLAN.													
ipv6-multicast	Use IPv6 multicast addressing over the VXLAN.													
learn-from-traffic	Enable/disable VXLAN MAC learning from traffic.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable VXLAN MAC learning from traffic.</td></tr><tr><td>disable</td><td>Disable VXLAN MAC learning from traffic.</td></tr></table>	Option	Description	enable	Enable VXLAN MAC learning from traffic.	disable	Disable VXLAN MAC learning from traffic.							
Option	Description													
enable	Enable VXLAN MAC learning from traffic.													
disable	Disable VXLAN MAC learning from traffic.													
multicast-ttl	VXLAN multicast TTL (1-255, default = 0).	integer	Minimum value: 1 Maximum value: 255	0										
name	VXLAN device or interface name. Must be a unique interface name.	string	Maximum length: 15											
remote-ip <ip>	IPv4 address of the VXLAN interface on the device at the remote end of the VXLAN. IPv4 address.	string	Maximum length: 15											
remote-ip6 <ip6>	IPv6 IP address of the VXLAN interface on the device at the remote end of the VXLAN. IPv6 address.	string	Maximum length: 45											
vni	VXLAN network ID.	integer	Minimum value: 1 Maximum value: 16777215	0										

config system wccp

Configure WCCP.

```
config system wccp
  Description: Configure WCCP.
```

```

edit <service-id>
  set assignment-bucket-format [wccp-v2|cisco-implementation]
  set assignment-dstaddr-mask {ipv4-netmask-any}
  set assignment-method [HASH|MASK|...]
  set assignment-srcaddr-mask {ipv4-netmask-any}
  set assignment-weight {integer}
  set authentication [enable|disable]
  set cache-engine-method [GRE|L2]
  set cache-id {ipv4-address}
  set forward-method [GRE|L2|...]
  set group-address {ipv4-address-multicast}
  set password {password}
  set ports {user}
  set ports-defined [source|destination]
  set primary-hash {option1}, {option2}, ...
  set priority {integer}
  set protocol {integer}
  set return-method [GRE|L2|...]
  set router-id {ipv4-address}
  set router-list {user}
  set server-list {user}
  set server-type [forward|proxy]
  set service-type [auto|standard|...]
next
end

```

config system wccp

Parameter	Description	Type	Size	Default
assignment-bucket-format	Assignment bucket format for the WCCP cache engine.	option	-	cisco-implementation
	Option	Description		
	wccp-v2	WCCP-v2 bucket format.		
	cisco-implementation	Cisco bucket format.		
assignment-dstaddr-mask	Assignment destination address mask.	ipv4-netmask-any	Not Specified	0.0.0.0
assignment-method	Hash key assignment preference.	option	-	HASH
	Option	Description		
	HASH	HASH assignment method.		
	MASK	MASK assignment method.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>HASH or MASK.</td></tr></table>	Option	Description	<i>any</i>	HASH or MASK.							
	Option	Description										
<i>any</i>	HASH or MASK.											
assignment-srcaddr-mask	Assignment source address mask.	ipv4-netmask-any	Not Specified	0.0.23.65								
assignment-weight	Assignment of hash weight/ratio for the WCCP cache engine.	integer	Minimum value: 0 Maximum value: 255	0								
authentication	Enable/disable MD5 authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MD5 authentication.</td></tr><tr><td><i>disable</i></td><td>Disable MD5 authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable MD5 authentication.	<i>disable</i>	Disable MD5 authentication.					
	Option	Description										
	<i>enable</i>	Enable MD5 authentication.										
<i>disable</i>	Disable MD5 authentication.											
cache-engine-method	Method used to forward traffic to the routers or to return to the cache engine.	option	-	GRE								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>GRE</i></td><td>GRE encapsulation.</td></tr><tr><td><i>L2</i></td><td>L2 rewrite.</td></tr></table>	Option	Description	<i>GRE</i>	GRE encapsulation.	<i>L2</i>	L2 rewrite.					
	Option	Description										
	<i>GRE</i>	GRE encapsulation.										
<i>L2</i>	L2 rewrite.											
cache-id	IP address known to all routers. If the addresses are the same, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0								
forward-method	Method used to forward traffic to the cache servers.	option	-	GRE								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>GRE</i></td><td>GRE encapsulation.</td></tr><tr><td><i>L2</i></td><td>L2 rewrite.</td></tr><tr><td><i>any</i></td><td>GRE or L2.</td></tr></table>	Option	Description	<i>GRE</i>	GRE encapsulation.	<i>L2</i>	L2 rewrite.	<i>any</i>	GRE or L2.			
	Option	Description										
	<i>GRE</i>	GRE encapsulation.										
	<i>L2</i>	L2 rewrite.										
<i>any</i>	GRE or L2.											
group-address	IP multicast address used by the cache routers. For the FortiGate to ignore multicast WCCP traffic, use the default 0.0.0.0.	ipv4-address-multicast	Not Specified	0.0.0.0								
password	Password for MD5 authentication.	password	Not Specified									

Parameter	Description	Type	Size	Default
ports	Service ports.	user	Not Specified	
ports-defined	Match method.	option	-	
	Option	Description		
	source	Source port match.		
	destination	Destination port match.		
primary-hash	Hash method.	option	-	dst-ip
	Option	Description		
	src-ip	Source IP hash.		
	dst-ip	Destination IP hash.		
	src-port	Source port hash.		
	dst-port	Destination port hash.		
priority	Service priority.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Service protocol.	integer	Minimum value: 0 Maximum value: 255	0
return-method	Method used to decline a redirected packet and return it to the FortiGate unit.	option	-	GRE
	Option	Description		
	GRE	GRE encapsulation.		
	L2	L2 rewrite.		
	any	GRE or L2.		
router-id	IP address known to all cache engines. If all cache engines connect to the same FortiGate interface, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0
router-list	IP addresses of one or more WCCP routers.	user	Not Specified	

Parameter	Description	Type	Size	Default								
server-list	IP addresses and netmasks for up to four cache servers.	user	Not Specified									
server-type	Cache server type.	option	-	forward								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward server.</td></tr><tr><td><i>proxy</i></td><td>Proxy server.</td></tr></table>	Option	Description	<i>forward</i>	Forward server.	<i>proxy</i>	Proxy server.					
Option	Description											
<i>forward</i>	Forward server.											
<i>proxy</i>	Proxy server.											
service-id	Service ID.	string	Maximum length: 3									
service-type	WCCP service type used by the cache server for logical interception and redirection of traffic.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>auto</td></tr><tr><td><i>standard</i></td><td>Standard service.</td></tr><tr><td><i>dynamic</i></td><td>Dynamic service.</td></tr></table>	Option	Description	<i>auto</i>	auto	<i>standard</i>	Standard service.	<i>dynamic</i>	Dynamic service.			
Option	Description											
<i>auto</i>	auto											
<i>standard</i>	Standard service.											
<i>dynamic</i>	Dynamic service.											

config system wireless ap-status



This command is available for model(s): FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure accepted wireless AP.

```
config system wireless ap-status
  Description: Configure accepted wireless AP.
  edit <id>
    set bssid {mac-address}
    set ssid {string}
    set status [rogue|accepted|...]
  next
end
```

config system wireless ap-status

Parameter	Description	Type	Size	Default
bssid	AP's BSSID.	mac-address	Not Specified	00:00:00:00:00:00

Parameter	Description	Type	Size	Default								
id	AP ID.	integer	Minimum value: 0 Maximum value: 4294967295									
ssid	AP's ssid	string	Maximum length: 32									
status	AP status.	option	-	rogue								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rogue</i></td><td>Rogue.</td></tr><tr><td><i>accepted</i></td><td>Accepted.</td></tr><tr><td><i>suppressed</i></td><td>Suppressed.</td></tr></table>				Option	Description	<i>rogue</i>	Rogue.	<i>accepted</i>	Accepted.	<i>suppressed</i>	Suppressed.
	Option	Description										
	<i>rogue</i>	Rogue.										
	<i>accepted</i>	Accepted.										
<i>suppressed</i>	Suppressed.											

config system wireless settings



This command is available for model(s): FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Wireless radio configuration.

```

config system wireless settings
    Description: Wireless radio configuration.
    set band [802.11a|802.11b|...]
    set beacon-interval {integer}
    set bgscan [disable|enable]
    set bgscan-idle {integer}
    set bgscan-interval {integer}
    set channel {integer}
    set channel-bonding [enable|disable]
    set geography [World|Americas|...]
    set mode [CLIENT|AP|...]
    set power-level {integer}
    set rogue-scan [enable|disable]
    set rogue-scan-mac-adjacency {integer}
    set short-guard-interval [enable|disable]
end

```

config system wireless settings

Parameter	Description	Type	Size	Default																										
band	Band.	option	-	802.11g																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g.</td></tr><tr><td>802.11g-only</td><td>802.11g only.</td></tr><tr><td>802.11n</td><td>802.11n at 2.4G band.</td></tr><tr><td>802.11ng-only</td><td>802.11ng only at 2.4G band.</td></tr><tr><td>802.11n-only</td><td>802.11n only at 2.4G band.</td></tr><tr><td>802.11n-5G</td><td>802.11n at 5G band.</td></tr><tr><td>802.11n-5G-only</td><td>802.11n only at 5G band.</td></tr><tr><td>802.11ac</td><td>802.11ac at 5G band.</td></tr><tr><td>802.11acn-only</td><td>802.11acn only at 5G band.</td></tr><tr><td>802.11ac-only</td><td>802.11ac only at 5G band.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g.	802.11g-only	802.11g only.	802.11n	802.11n at 2.4G band.	802.11ng-only	802.11ng only at 2.4G band.	802.11n-only	802.11n only at 2.4G band.	802.11n-5G	802.11n at 5G band.	802.11n-5G-only	802.11n only at 5G band.	802.11ac	802.11ac at 5G band.	802.11acn-only	802.11acn only at 5G band.	802.11ac-only	802.11ac only at 5G band.			
	Option	Description																												
	802.11a	802.11a.																												
	802.11b	802.11b.																												
	802.11g	802.11g.																												
	802.11g-only	802.11g only.																												
	802.11n	802.11n at 2.4G band.																												
	802.11ng-only	802.11ng only at 2.4G band.																												
	802.11n-only	802.11n only at 2.4G band.																												
	802.11n-5G	802.11n at 5G band.																												
	802.11n-5G-only	802.11n only at 5G band.																												
	802.11ac	802.11ac at 5G band.																												
	802.11acn-only	802.11acn only at 5G band.																												
802.11ac-only	802.11ac only at 5G band.																													
beacon-interval	Beacon level (25 - 1000).	integer	Minimum value: 25 Maximum value: 1000	100																										
bgscan	Enable/disable background rogue AP scan.	option	-	disable																										

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable background rogue AP scan.		
	<i>enable</i>	Enable background rogue AP scan.		
bgscan-idle	Interval between scanning channels (100 - 1000 ms).	integer	Minimum value: 100 Maximum value: 1000	250
bgscan-interval	Interval between two rounds of scanning (15 - 3600 sec).	integer	Minimum value: 15 Maximum value: 3600	120
channel	Channel.	integer	Minimum value: 0 Maximum value: 4294967295	0
channel-bonding	Supported channel width.	option	-	disable
	Option Description			
	<i>enable</i>	20/40 MHz.		
	<i>disable</i>	20 MHz.		
geography	Geography.	option	-	Americas
	Option Description			
	<i>World</i>	World.		
	<i>Americas</i>	Americas.		
	<i>EMEA</i>	EMEA.		
	<i>Israel</i>	Israel.		
	<i>Japan</i>	Japan.		
mode	Mode.	option	-	AP
	Option Description			
	<i>CLIENT</i>	Client.		
	<i>AP</i>	Access point.		
	<i>SCAN</i>	Scan.		

Parameter	Description	Type	Size	Default						
power-level	Power level (0 - 17).	integer	Minimum value: 0 Maximum value: 17	17						
rogue-scan	Enable/disable rogue scan.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable rogue scan.</td></tr><tr><td>disable</td><td>Disable rogue scan.</td></tr></table>				Option	Description	enable	Enable rogue scan.	disable	Disable rogue scan.
	Option	Description								
	enable	Enable rogue scan.								
disable	Disable rogue scan.									
rogue-scan-mac-adjacency	MAC adjacency (0-31).	integer	Minimum value: 0 Maximum value: 31	7						
short-guard-interval	Enable/disable short guard interval.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>400 ns long guard interval.</td></tr><tr><td>disable</td><td>800 ns short guard interval.</td></tr></table>				Option	Description	enable	400 ns long guard interval.	disable	800 ns short guard interval.
	Option	Description								
	enable	400 ns long guard interval.								
disable	800 ns short guard interval.									

config system zone

Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual interfaces in the zone.

```
config system zone
    Description: Configure zones to group two or more interfaces. When a zone is created you can
    configure policies for the zone instead of individual interfaces in the zone.
    edit <name>
        set description {string}
        set interface <interface-name1>, <interface-name2>, ...
        set intrazone [allow|deny]
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
    next
end
```

config system zone

Parameter	Description	Type	Size	Default						
description	Description.	string	Maximum length: 127							
interface <interface-name>	Add interfaces to this zone. Interfaces must not be assigned to another zone or have firewall policies defined. Select interfaces to add to the zone.	string	Maximum length: 79							
intrazone	Allow or deny traffic routing between different interfaces in the same zone (default = deny).	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow traffic between interfaces in the zone.</td></tr><tr><td>deny</td><td>Deny traffic between interfaces in the zone.</td></tr></table>				Option	Description	allow	Allow traffic between interfaces in the zone.	deny	Deny traffic between interfaces in the zone.
Option	Description									
allow	Allow traffic between interfaces in the zone.									
deny	Deny traffic between interfaces in the zone.									
name	Zone name.	string	Maximum length: 35							

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
name	Tagging entry name.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

telemetry-controller

This section includes syntax for the following commands:

- [config telemetry-controller agent-profile on page 2006](#)
- [config telemetry-controller agent on page 2004](#)
- [config telemetry-controller application predefine on page 2007](#)
- [config telemetry-controller global on page 2008](#)
- [config telemetry-controller profile on page 2009](#)

config telemetry-controller agent



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure FortiTelemetry agents managed by a FortiGate unit.

```
config telemetry-controller agent
  Description: Configure FortiTelemetry agents managed by a FortiGate unit.
  edit <agent-id>
    set agent-profile {string}
    set alias {string}
    set authz [rejected|authorized|...]
```

```
        set comment {var-string}
    next
end
```

config telemetry-controller agent

Parameter	Description	Type	Size	Default
agent-id	Agent ID.	string	Maximum length: 19	
agent-profile	Name of an existing agent profile.	string	Maximum length: 35	
alias	Alias used in display for ease of distinguishing agents.	string	Maximum length: 35	
authz	Authorization status of this agent.	option	-	unauthorized
	Option Description			
	<i>rejected</i>	Agent is rejected.		
	<i>authorized</i>	Agent is authorized.		
	<i>unauthorized</i>	Agent is unauthorized.		
comment	Comment.	var-string	Maximum length: 255	

config telemetry-controller agent-profile



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure FortiTelemetry agent profiles.

```
config telemetry-controller agent-profile
  Description: Configure FortiTelemetry agent profiles.
  edit <name>
    set comment {var-string}
    set model [FTL100G|WINDOWS]
  next
end
```

config telemetry-controller agent-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
model	Model.	option	-	FTL100G

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>FTL100G</i>	FTL100G.		
	<i>WINDOWS</i>	WINDOWS.		
name	Name of the agent profile.	string	Maximum length: 35	

config telemetry-controller application predefine



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure FortiTelemetry predefined applications.

```
config telemetry-controller application predefine
    Description: Configure FortiTelemetry predefined applications.
    edit <app-name>
        set comment {var-string}
    next
end
```

config telemetry-controller application predefine

Parameter	Description	Type	Size	Default
app-name	Application name.	string	Maximum length: 79	
comment	Comment. Read-only.	var-string	Maximum length: 255	

config telemetry-controller global



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure FortiTelemetry global settings.

```
config telemetry-controller global
  Description: Configure FortiTelemetry global settings.
  set region {option}
  set retry-interval {integer}
  set telemetry-ca-certificate {string}
end
```


config telemetry-controller global

Parameter	Description	Type	Size	Default				
region	Configure telemetry cloud region.	option	-	global				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Set region to gloabl.</td></tr></table>	Option	Description	<i>global</i>	Set region to gloabl.			
	Option	Description						
<i>global</i>	Set region to gloabl.							
retry-interval	Configure telemetry cloud retry interval (1 - 999, default = 60).	integer	Minimum value: 1 Maximum value: 999	60				
telemetry-ca-certificate	Name of the CA certificate used to verify the telemetry agent certificate.	string	Maximum length: 79					

config telemetry-controller profile



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate 90G, FortiGate 91G, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure FortiTelemetry profiles.

```
config telemetry-controller profile
  Description: Configure FortiTelemetry profiles.
  edit <name>
```

```

config application
    Description: Configure applications.
    edit <id>
        set app-name {string}
        set interval {integer}
        set monitor [enable|disable]
        config sla
            Description: Service level agreement (SLA).
            set app-throughput-threshold {integer}
            set atdt-threshold {integer}
            set dns-time-threshold {integer}
            set experience-score-threshold {integer}
            set failure-rate-threshold {integer}
            set jitter-threshold {integer}
            set latency-threshold {integer}
            set packet-loss-threshold {integer}
            set sla-factor {option1}, {option2}, ...
            set tcp-rtt-threshold {integer}
            set tls-time-threshold {integer}
            set ttfb-threshold {integer}
        end
    end
next
end
set comment {var-string}
next
end

```

config telemetry-controller profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Name of the profile.	string	Maximum length: 35	

config application

Parameter	Description	Type	Size	Default
app-name	Application name.	string	Maximum length: 79	
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default						
interval	Time in milliseconds to check the application (1000 - 86,400 * 1000, default = 300 * 1000 ms).	integer	Minimum value: 1000 Maximum value: 86400000	300000						
monitor	Enable/disable monitoring of the application.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable monitoring of the application.</td></tr><tr><td><i>disable</i></td><td>Disable monitoring of the application.</td></tr></table>				Option	Description	<i>enable</i>	Enable monitoring of the application.	<i>disable</i>	Disable monitoring of the application.
Option	Description									
<i>enable</i>	Enable monitoring of the application.									
<i>disable</i>	Disable monitoring of the application.									

config sla

Parameter	Description	Type	Size	Default
app-throughput-threshold	Threshold of application throughput in megabytes (0 - 10,000, default = 2 MB).	integer	Minimum value: 0 Maximum value: 10000	2
atdt-threshold	Threshold of application total downloading time in milliseconds (0 - 10,000,000, default = 3,000 ms).	integer	Minimum value: 0 Maximum value: 10000000	3000
dns-time-threshold	Threshold of 95th percentile of DNS resolution time in milliseconds (0 - 10,000,000, default = 100 ms).	integer	Minimum value: 0 Maximum value: 10000000	100
experience-score-threshold	Threshold of experience score (0 - 10, default = 6).	integer	Minimum value: 0 Maximum value: 10	6
failure-rate-threshold	Threshold of failure rate (0 - 100, default = 5 percentage).	integer	Minimum value: 0 Maximum value: 100	5
jitter-threshold	Threshold of jitter in milliseconds (0 - 10,000,000, default = 50 ms).	integer	Minimum value: 0 Maximum value: 10000000	50

Parameter	Description	Type	Size	Default																								
latency-threshold	Threshold of latency in milliseconds (0 - 10,000,000, default = 100 ms).	integer	Minimum value: 0 Maximum value: 10000000	100																								
packet-loss-threshold	Threshold of packet loss (0 - 100, default = 5 percentage).	integer	Minimum value: 0 Maximum value: 100	5																								
sla-factor	Criteria on which metric to SLA threshold list.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>experience-score</i></td><td>Select SLA target based on experience score.</td></tr><tr><td><i>failure-rate</i></td><td>Select SLA target based on failure rate.</td></tr><tr><td><i>latency</i></td><td>Select SLA target based on latency.</td></tr><tr><td><i>jitter</i></td><td>Select SLA target based on jitter.</td></tr><tr><td><i>packet-loss</i></td><td>Select SLA target based on packet loss.</td></tr><tr><td><i>tftb</i></td><td>Select SLA target based on time to first byte.</td></tr><tr><td><i>atdt</i></td><td>Select SLA target based on application total downloading time.</td></tr><tr><td><i>tcp-rtt</i></td><td>Select SLA target based on TCP round-trip time.</td></tr><tr><td><i>dns-time</i></td><td>Select SLA target based on DNS resolution time.</td></tr><tr><td><i>tls-time</i></td><td>Select SLA target based on TLS handshake time.</td></tr><tr><td><i>app-throughput</i></td><td>Select SLA target based on application throughput.</td></tr></table>				Option	Description	<i>experience-score</i>	Select SLA target based on experience score.	<i>failure-rate</i>	Select SLA target based on failure rate.	<i>latency</i>	Select SLA target based on latency.	<i>jitter</i>	Select SLA target based on jitter.	<i>packet-loss</i>	Select SLA target based on packet loss.	<i>tftb</i>	Select SLA target based on time to first byte.	<i>atdt</i>	Select SLA target based on application total downloading time.	<i>tcp-rtt</i>	Select SLA target based on TCP round-trip time.	<i>dns-time</i>	Select SLA target based on DNS resolution time.	<i>tls-time</i>	Select SLA target based on TLS handshake time.	<i>app-throughput</i>	Select SLA target based on application throughput.
Option	Description																											
<i>experience-score</i>	Select SLA target based on experience score.																											
<i>failure-rate</i>	Select SLA target based on failure rate.																											
<i>latency</i>	Select SLA target based on latency.																											
<i>jitter</i>	Select SLA target based on jitter.																											
<i>packet-loss</i>	Select SLA target based on packet loss.																											
<i>tftb</i>	Select SLA target based on time to first byte.																											
<i>atdt</i>	Select SLA target based on application total downloading time.																											
<i>tcp-rtt</i>	Select SLA target based on TCP round-trip time.																											
<i>dns-time</i>	Select SLA target based on DNS resolution time.																											
<i>tls-time</i>	Select SLA target based on TLS handshake time.																											
<i>app-throughput</i>	Select SLA target based on application throughput.																											
tcp-rtt-threshold	Threshold of TCP round-trip time in milliseconds (0 - 10,000,000, default = 100 ms).	integer	Minimum value: 0 Maximum value: 10000000	100																								
tls-time-threshold	Threshold of 95th percentile of TLS handshake time in milliseconds (0 - 10,000,000, default = 200 ms).	integer	Minimum value: 0 Maximum value: 10000000	200																								
tftb-threshold	Threshold of time to first byte in milliseconds (0 - 10,000,000, default = 200 ms).	integer	Minimum value: 0 Maximum value: 10000000	200																								

user

This section includes syntax for the following commands:

- [config user adgrp on page 2013](#)
- [config user certificate on page 2014](#)
- [config user domain-controller on page 2015](#)
- [config user exchange on page 2019](#)
- [config user external-identity-provider on page 2021](#)
- [config user fortitoken on page 2023](#)
- [config user fsso-polling on page 2028](#)
- [config user fsso on page 2024](#)
- [config user group on page 2030](#)
- [config user krb-keytab on page 2035](#)
- [config user ldap on page 2036](#)
- [config user local on page 2045](#)
- [config user nac-policy on page 2048](#)
- [config user password-policy on page 2051](#)
- [config user peer on page 2053](#)
- [config user peergrp on page 2055](#)
- [config user pop3 on page 2056](#)
- [config user quarantine on page 2057](#)
- [config user radius on page 2058](#)
- [config user saml on page 2074](#)
- [config user scim on page 2078](#)
- [config user security-exempt-list on page 2080](#)
- [config user setting on page 2081](#)
- [config user tacacs+ on page 2086](#)

config user adgrp

Configure FSSO groups.

```
config user adgrp
  Description: Configure FSSO groups.
  edit <name>
    set connector-source {string}
    set id {integer}
    set server-name {string}
```

```
next
end
```

config user adgrp

Parameter	Description	Type	Size	Default
connector-source	FSSO connector source.	string	Maximum length: 35	
id	Group ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Name.	string	Maximum length: 511	
server-name	FSSO agent name.	string	Maximum length: 35	

config user certificate

Configure certificate users.

```
config user certificate
  Description: Configure certificate users.
  edit <name>
    set common-name {string}
    set id {integer}
    set issuer {string}
    set status [enable|disable]
    set type [single-certificate|trusted-issuer]
  next
end
```

config user certificate

Parameter	Description	Type	Size	Default
common-name	Certificate common name.	string	Maximum length: 64	
id	User ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default						
issuer	CA certificate used for client certificate verification.	string	Maximum length: 79							
name	User name.	string	Maximum length: 64							
status	Enable/disable allowing the certificate user to authenticate with the FortiGate unit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user.</td></tr><tr><td><i>disable</i></td><td>Disable user.</td></tr></table>				Option	Description	<i>enable</i>	Enable user.	<i>disable</i>	Disable user.
Option	Description									
<i>enable</i>	Enable user.									
<i>disable</i>	Disable user.									
type	Type of certificate authentication method.	option	-	single-certificate						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single-certificate</i></td><td>Single certificate.</td></tr><tr><td><i>trusted-issuer</i></td><td>Trusted CA issuer.</td></tr></table>				Option	Description	<i>single-certificate</i>	Single certificate.	<i>trusted-issuer</i>	Trusted CA issuer.
Option	Description									
<i>single-certificate</i>	Single certificate.									
<i>trusted-issuer</i>	Trusted CA issuer.									

config user domain-controller

Configure domain controller entries.

```

config user domain-controller
  Description: Configure domain controller entries.
  edit <name>
    set ad-mode [none|ds|...]
    set adlds-dn {string}
    set adlds-ip-address {ipv4-address}
    set adlds-ip6 {ipv6-address}
    set adlds-port {integer}
    set change-detection [enable|disable]
    set change-detection-period {integer}
    set dns-srv-lookup [enable|disable]
    set domain-name {string}
    config extra-server
      Description: Extra servers.
      edit <id>
        set ip-address {ipv4-address}
        set port {integer}
        set source-ip-address {ipv4-address}
        set source-port {integer}
      next
    end
  end

```

```

set hostname {string}
set interface {string}
set interface-select-method [auto|sdwan|...]
set ip-address {ipv4-address}
set ip6 {ipv6-address}
set ldap-server <name1>, <name2>, ...
set password {password}
set port {integer}
set replication-port {integer}
set source-ip-address {ipv4-address}
set source-ip6 {ipv6-address}
set source-port {integer}
set username {string}
next
end

```

config user domain-controller

Parameter	Description	Type	Size	Default
ad-mode	Set Active Directory mode.	option	-	none
	Option	Description		
	<i>none</i>	The server is not configured as an Active Directory Domain Server (AD DS).		
	<i>ds</i>	The server is configured as an Active Directory Domain Server (AD DS).		
	<i>lds</i>	The server is an Active Directory Lightweight Domain Server (AD LDS).		
adlds-dn	AD LDS distinguished name.	string	Maximum length: 255	
adlds-ip-address	AD LDS IPv4 address.	ipv4-address	Not Specified	0.0.0.0
adlds-ip6	AD LDS IPv6 address.	ipv6-address	Not Specified	::
adlds-port	Port number of AD LDS service (default = 389).	integer	Minimum value: 0 Maximum value: 65535	389
change-detection	Enable/disable detection of a configuration change in the Active Directory server.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable detection of a configuration change in the Active Directory server.</td></tr><tr><td><i>disable</i></td><td>Disable detection of a configuration change in the Active Directory server.</td></tr></table>	Option	Description	<i>enable</i>	Enable detection of a configuration change in the Active Directory server.	<i>disable</i>	Disable detection of a configuration change in the Active Directory server.					
	Option	Description										
	<i>enable</i>	Enable detection of a configuration change in the Active Directory server.										
<i>disable</i>	Disable detection of a configuration change in the Active Directory server.											
change-detection-period	Minutes to detect a configuration change in the Active Directory server (5 - 10080 minutes (7 days), default = 60).	integer	Minimum value: 5 Maximum value: 10080	60								
dns-srv-lookup	Enable/disable DNS service lookup.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DNS service lookup.</td></tr><tr><td><i>disable</i></td><td>Disable DNS service lookup.</td></tr></table>	Option	Description	<i>enable</i>	Enable DNS service lookup.	<i>disable</i>	Disable DNS service lookup.					
	Option	Description										
	<i>enable</i>	Enable DNS service lookup.										
<i>disable</i>	Disable DNS service lookup.											
domain-name	Domain DNS name.	string	Maximum length: 255									
hostname	Hostname of the server to connect to.	string	Maximum length: 255									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
ip-address	Domain controller IPv4 address.	ipv4-address	Not Specified	0.0.0.0								
ip6	Domain controller IPv6 address.	ipv6-address	Not Specified	::								
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default
name	Domain controller entry name.	string	Maximum length: 35	
password	Password for specified username.	password	Not Specified	
port	Port to be used for communication with the domain controller (default = 445).	integer	Minimum value: 0 Maximum value: 65535	445
replication-port	Port to be used for communication with the domain controller for replication service. Port number 0 indicates automatic discovery.	integer	Minimum value: 0 Maximum value: 65535	0
source-ip-address	FortiGate IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0
source-ip6	FortiGate IPv6 address to be used for communication with the domain controller.	ipv6-address	Not Specified	::
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0
username	User name to sign in with. Must have proper permissions for service.	string	Maximum length: 64	

config extra-server

Parameter	Description	Type	Size	Default
id	Server ID.	integer	Minimum value: 1 Maximum value: 100	0
ip-address	Domain controller IP address.	ipv4-address	Not Specified	0.0.0.0
port	Port to be used for communication with the domain controller (default = 445).	integer	Minimum value: 0 Maximum value: 65535	445

Parameter	Description	Type	Size	Default
source-ip-address	FortiGate IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0

config user exchange

Configure MS Exchange server entries.

```

config user exchange
  Description: Configure MS Exchange server entries.
  edit <name>
    set auth-level [connect|call|...]
    set auth-type [spnego|ntlm|...]
    set auto-discover-kdc [enable|disable]
    set connect-protocol [rpc-over-tcp|rpc-over-http|...]
    set domain-name {string}
    set http-auth-type [basic|ntlm]
    set ip {ipv4-address-any}
    set kdc-ip <ipv41>, <ipv42>, ...
    set password {password}
    set server-name {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set username {string}
    set validate-server-certificate [disable|enable]
  next
end

```

config user exchange

Parameter	Description	Type	Size	Default
auth-level	Authentication security level used for the RPC protocol layer.	option	-	privacy
	Option	Description		
	connect	RPC authentication level 'connect'.		
	call	RPC authentication level 'call'.		
	packet	RPC authentication level 'packet'.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>integrity</i></td><td>RPC authentication level 'integrity'.</td></tr><tr><td><i>privacy</i></td><td>RPC authentication level 'privacy'.</td></tr></table>	Option	Description	<i>integrity</i>	RPC authentication level 'integrity'.	<i>privacy</i>	RPC authentication level 'privacy'.					
Option	Description											
<i>integrity</i>	RPC authentication level 'integrity'.											
<i>privacy</i>	RPC authentication level 'privacy'.											
auth-type	Authentication security type used for the RPC protocol layer.	option	-	kerberos								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>spnego</i></td><td>Negotiate authentication.</td></tr><tr><td><i>ntlm</i></td><td>NTLM authentication.</td></tr><tr><td><i>kerberos</i></td><td>Kerberos authentication.</td></tr></table>	Option	Description	<i>spnego</i>	Negotiate authentication.	<i>ntlm</i>	NTLM authentication.	<i>kerberos</i>	Kerberos authentication.			
Option	Description											
<i>spnego</i>	Negotiate authentication.											
<i>ntlm</i>	NTLM authentication.											
<i>kerberos</i>	Kerberos authentication.											
auto-discover-kdc	Enable/disable automatic discovery of KDC IP addresses.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic discovery of KDC IP addresses.</td></tr><tr><td><i>disable</i></td><td>Disable automatic discovery of KDC IP addresses.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic discovery of KDC IP addresses.	<i>disable</i>	Disable automatic discovery of KDC IP addresses.					
Option	Description											
<i>enable</i>	Enable automatic discovery of KDC IP addresses.											
<i>disable</i>	Disable automatic discovery of KDC IP addresses.											
connect-protocol	Connection protocol used to connect to MS Exchange service.	option	-	rpc-over-https								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rpc-over-tcp</i></td><td>Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.</td></tr><tr><td><i>rpc-over-http</i></td><td>Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.</td></tr><tr><td><i>rpc-over-https</i></td><td>Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.</td></tr></table>	Option	Description	<i>rpc-over-tcp</i>	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.	<i>rpc-over-http</i>	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.	<i>rpc-over-https</i>	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.			
Option	Description											
<i>rpc-over-tcp</i>	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.											
<i>rpc-over-http</i>	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.											
<i>rpc-over-https</i>	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.											
domain-name	MS Exchange server fully qualified domain name.	string	Maximum length: 79									
http-auth-type	Authentication security type used for the HTTP transport.	option	-	ntlm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>basic</i></td><td>Basic HTTP authentication.</td></tr><tr><td><i>ntlm</i></td><td>NTLM HTTP authentication.</td></tr></table>	Option	Description	<i>basic</i>	Basic HTTP authentication.	<i>ntlm</i>	NTLM HTTP authentication.					
Option	Description											
<i>basic</i>	Basic HTTP authentication.											
<i>ntlm</i>	NTLM HTTP authentication.											

Parameter	Description	Type	Size	Default														
ip	Server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0														
kdc-ip <ipv4>	KDC IPv4 addresses for Kerberos authentication. KDC IPv4 addresses for Kerberos authentication.	string	Maximum length: 79															
name	MS Exchange server entry name.	string	Maximum length: 35															
password	Password for the specified username.	password	Not Specified															
server-name	MS Exchange server hostname.	string	Maximum length: 63															
ssl-min-proto-version	Minimum SSL/TLS protocol version for HTTPS transport (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>				Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
username	User name used to sign in to the server. Must have proper permissions for service.	string	Maximum length: 64															
validate-server-certificate	Enable/disable exchange server certificate validation.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable validation of server certificate.</td></tr><tr><td>enable</td><td>Enable validation of server certificate.</td></tr></table>				Option	Description	disable	Disable validation of server certificate.	enable	Enable validation of server certificate.								
Option	Description																	
disable	Disable validation of server certificate.																	
enable	Enable validation of server certificate.																	

config user external-identity-provider

Configure external identity provider.

```

config user external-identity-provider
  Description: Configure external identity provider.
  edit <name>
    set group-attr-name {string}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set port {integer}
    set server-identity-check [disable|enable]
    set source-ip {string}
    set timeout {integer}
    set type {option}
    set url {string}
    set user-attr-name {string}
    set version [v1.0|beta]
    set vrf-select {integer}
  next
end

```

config user external-identity-provider

Parameter	Description	Type	Size	Default								
group-attr-name	Group attribute name in authentication query.	string	Maximum length: 63	id								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
	Option	Description										
	auto	Set outgoing interface automatically.										
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.										
specify	Set outgoing interface manually.											
name	External identity provider name.	string	Maximum length: 35									
port	External identity provider service port number (0 to use default).	integer	Minimum value: 0 Maximum value: 65535	0								
server-identity-check	Enable/disable server's identity check against its certificate and subject alternative name(s).	option	-	enable								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not check server's identity against its certificate and subject alternative name(s).</td></tr><tr><td><i>enable</i></td><td>Check server's identity against its certificate and subject alternative name(s).</td></tr></table>				Option	Description	<i>disable</i>	Do not check server's identity against its certificate and subject alternative name(s).	<i>enable</i>	Check server's identity against its certificate and subject alternative name(s).
	Option	Description								
	<i>disable</i>	Do not check server's identity against its certificate and subject alternative name(s).								
<i>enable</i>	Check server's identity against its certificate and subject alternative name(s).									
source-ip	Use this IPv4/v6 address to connect to the external identity provider.	string	Maximum length: 63							
timeout	Connection timeout value in seconds (default=5).	integer	Minimum value: 1 Maximum value: 60	5						
type	External identity provider type.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ms-graph</i></td><td>Microsoft Graph server.</td></tr></table>				Option	Description	<i>ms-graph</i>	Microsoft Graph server.		
	Option	Description								
<i>ms-graph</i>	Microsoft Graph server.									
url	External identity provider URL (e.g. "https://example.com:8080/api/v1"). Read-only.	string	Maximum length: 127							
user-attr-name	User attribute name in authentication query.	string	Maximum length: 63	userPrincipalName						
version	External identity API version.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>v1.0</i></td><td>MS Graph REST API v1.0.</td></tr><tr><td><i>beta</i></td><td>MS Graph REST API beta (debug build only).</td></tr></table>				Option	Description	<i>v1.0</i>	MS Graph REST API v1.0.	<i>beta</i>	MS Graph REST API beta (debug build only).
	Option	Description								
	<i>v1.0</i>	MS Graph REST API v1.0.								
<i>beta</i>	MS Graph REST API beta (debug build only).									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config user fortitoken

Configure FortiToken.

```
config user fortitoken
  Description: Configure FortiToken.
  edit <serial-number>
    set activation-code {string}
```

```

        set activation-expire {integer}
        set comments {var-string}
        set license {string}
        set os-ver {string}
        set reg-id {string}
        set seed {string}
        set status [active|lock]
    next
end

```

config user fortitoken

Parameter	Description	Type	Size	Default
activation-code	Mobile token user activation-code.	string	Maximum length: 32	
activation-expire	Mobile token user activation-code expire time.	integer	Minimum value: 0 Maximum value: 4294967295	
comments	Comment.	var-string	Maximum length: 255	
license	Mobile token license.	string	Maximum length: 31	
os-ver	Device Mobile Version.	string	Maximum length: 15	
reg-id	Device Reg ID.	string	Maximum length: 256	
seed	Token seed.	string	Maximum length: 208	
serial-number	Serial number.	string	Maximum length: 16	
status	Status.	option	-	active
		Option	Description	
		active	Activate FortiToken.	
		lock	Lock FortiToken.	

config user fsso

Configure Fortinet Single Sign On (FSSO) agents.


```

config user fsso
  Description: Configure Fortinet Single Sign On (FSSO) agents.
  edit <name>
    set group-poll-interval {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ldap-poll [enable|disable]
    set ldap-poll-filter {string}
    set ldap-poll-interval {integer}
    set ldap-server {string}
    set logon-timeout {integer}
    set password {password}
    set password2 {password}
    set password3 {password}
    set password4 {password}
    set password5 {password}
    set port {integer}
    set port2 {integer}
    set port3 {integer}
    set port4 {integer}
    set port5 {integer}
    set server {string}
    set server2 {string}
    set server3 {string}
    set server4 {string}
    set server5 {string}
    set sni {string}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set ssl [enable|disable]
    set ssl-server-host-ip-check [enable|disable]
    set ssl-trusted-cert {string}
    set type [default|fortinac]
    set user-info-server {string}
    set vrf-select {integer}
  next
end

```

config user fsso

Parameter	Description	Type	Size	Default
group-poll-interval	Interval in minutes within to fetch groups from FSSO server, or unset to disable.	integer	Minimum value: 1 Maximum value: 2880	0
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
ldap-poll	Enable/disable automatic fetching of groups from LDAP server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatic fetching of groups from LDAP server.		
	<i>disable</i>	Disable automatic fetching of groups from LDAP server.		
ldap-poll-filter	Filter used to fetch groups.	string	Maximum length: 2047	(objectCategory=group)
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880	180
ldap-server	LDAP server to get group information.	string	Maximum length: 35	
logon-timeout	Interval in minutes to keep logons after FSSO server down.	integer	Minimum value: 1 Maximum value: 2880	5
name	Name.	string	Maximum length: 35	
password	Password of the first FSSO collector agent.	password	Not Specified	
password2	Password of the second FSSO collector agent.	password	Not Specified	
password3	Password of the third FSSO collector agent.	password	Not Specified	
password4	Password of the fourth FSSO collector agent.	password	Not Specified	

Parameter	Description	Type	Size	Default
password5	Password of the fifth FSSO collector agent.	password	Not Specified	
port	Port of the first FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
port2	Port of the second FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
port3	Port of the third FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
port5	Port of the fifth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
server	Domain name or IP address of the first FSSO collector agent.	string	Maximum length: 63	
server2	Domain name or IP address of the second FSSO collector agent.	string	Maximum length: 63	
server3	Domain name or IP address of the third FSSO collector agent.	string	Maximum length: 63	
server4	Domain name or IP address of the fourth FSSO collector agent.	string	Maximum length: 63	
server5	Domain name or IP address of the fifth FSSO collector agent.	string	Maximum length: 63	
sni	Server Name Indication.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
source-ip	Source IP for communications to FSSO agent.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	IPv6 source for communications to FSSO agent.	ipv6-address	Not Specified	::						
ssl	Enable/disable use of SSL.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of SSL.</td></tr><tr><td><i>disable</i></td><td>Disable use of SSL.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of SSL.	<i>disable</i>	Disable use of SSL.			
Option	Description									
<i>enable</i>	Enable use of SSL.									
<i>disable</i>	Disable use of SSL.									
ssl-server-host-ip-check	Enable/disable server host/IP verification.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server host/IP verification.</td></tr><tr><td><i>disable</i></td><td>Disable server host/IP verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable server host/IP verification.	<i>disable</i>	Disable server host/IP verification.			
Option	Description									
<i>enable</i>	Enable server host/IP verification.									
<i>disable</i>	Disable server host/IP verification.									
ssl-trusted-cert	Trusted server certificate or CA certificate.	string	Maximum length: 79							
type	Server type.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>All other unspecified types of servers.</td></tr><tr><td><i>fortinac</i></td><td>FortiNAC server.</td></tr></table>	Option	Description	<i>default</i>	All other unspecified types of servers.	<i>fortinac</i>	FortiNAC server.			
Option	Description									
<i>default</i>	All other unspecified types of servers.									
<i>fortinac</i>	FortiNAC server.									
user-info-server	LDAP server to get user information.	string	Maximum length: 35							
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config user fsso-polling

Configure FSSO active directory servers for polling mode.

```
config user fsso-polling
  Description: Configure FSSO active directory servers for polling mode.
  edit <id>
    config adgrp
```

```

        Description: LDAP Group Info.
        edit <name>
        next
    end
    set default-domain {string}
    set ldap-server {string}
    set logon-history {integer}
    set password {password}
    set polling-frequency {integer}
    set port {integer}
    set server {string}
    set smb-ntlmv1-auth [enable|disable]
    set smbv1 [enable|disable]
    set status [enable|disable]
    set user {string}
next
end

```

config user fsso-polling

Parameter	Description	Type	Size	Default
default-domain	Default domain managed by this Active Directory server.	string	Maximum length: 35	
id	Active Directory server ID.	integer	Minimum value: 0 Maximum value: 4294967295	
ldap-server	LDAP server name used in LDAP connection strings.	string	Maximum length: 35	
logon-history	Number of hours of logon history to keep, 0 means keep all history.	integer	Minimum value: 0 Maximum value: 48	8
password	Password required to log into this Active Directory server.	password	Not Specified	
polling-frequency	Polling frequency (every 1 to 30 seconds).	integer	Minimum value: 1 Maximum value: 30	10
port	Port to communicate with this Active Directory server.	integer	Minimum value: 0 Maximum value: 65535	0
server	Host name or IP address of the Active Directory server.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
smb-ntlmv1-auth	Enable/disable support of NTLMv1 for Samba authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable support of NTLMv1 for Samba authentication.		
	<i>disable</i>	Disable support of NTLMv1 for Samba authentication.		
smbv1	Enable/disable support of SMBv1 for Samba.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable support of SMBv1 for Samba.		
	<i>disable</i>	Disable support of SMBv1 for Samba.		
status	Enable/disable polling for the status of this Active Directory server.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
user	User name required to log into this Active Directory server.	string	Maximum length: 35	

config adgrp

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 511	

config user group

Configure user groups.

```
config user group
  Description: Configure user groups.
  edit <name>
    set auth-concurrent-override [enable|disable]
    set auth-concurrent-value {integer}
    set authtimeout {integer}
    set company [optional|mandatory|...]
    set email [disable|enable]
    set expire {integer}
```

```

set expire-type [immediately|first-successful-login]
set group-type [firewall|fsso-service|...]
config guest
    Description: Guest User.
    edit <id>
        set comment {var-string}
        set company {string}
        set email {string}
        set expiration {user}
        set mobile-phone {string}
        set name {string}
        set password {password}
        set sponsor {string}
        set user-id {string}
    next
end
set http-digest-realm {string}
set id {integer}
config match
    Description: Group matches.
    edit <id>
        set group-name {string}
        set server-name {string}
    next
end
set max-accounts {integer}
set member <name1>, <name2>, ...
set mobile-phone [disable|enable]
set multiple-guest-add [disable|enable]
set password [auto-generate|specify|...]
set sms-custom-server {string}
set sms-server [fortiguard|custom]
set sponsor [optional|mandatory|...]
set sso-attribute-value {string}
set user-id [email|auto-generate|...]
set user-name [disable|enable]
next
end

```

config user group

Parameter	Description	Type	Size	Default
auth-concurrent-override	Enable/disable overriding the global number of concurrent authentication sessions for this user group.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable auth-concurrent-override.		
	<i>disable</i>	Disable auth-concurrent-override.		
auth-concurrent-value	Maximum number of concurrent authenticated connections per user (0 - 100).	integer	Minimum value: 0 0 Maximum value: 100	
authtimeout	Authentication timeout in minutes for this user group. 0 to use the global user setting auth-timeout.	integer	Minimum value: 0 0 Maximum value: 43200	
company	Set the action for the company guest user field.	option	-	optional
	Option Description			
	<i>optional</i>	Optional.		
	<i>mandatory</i>	Mandatory.		
	<i>disabled</i>	Disabled.		
email	Enable/disable the guest user email address field.	option	-	enable
	Option Description			
	<i>disable</i>	Disable setting.		
	<i>enable</i>	Enable setting.		
expire	Time in seconds before guest user accounts expire (1 - 31536000).	integer	Minimum value: 14400 1 Maximum value: 31536000	
expire-type	Determine when the expiration countdown begins.	option	-	immediately
	Option Description			
	<i>immediately</i>	Immediately.		
	<i>first-successful-login</i>	First successful login.		
group-type	Set the group to be for firewall authentication, FSSO, RSSO, or guest users.	option	-	firewall

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>firewall</i></td><td>Firewall.</td></tr><tr><td><i>fsso-service</i></td><td>Fortinet Single Sign-On Service.</td></tr><tr><td><i>rsso</i></td><td>RADIUS based Single Sign-On Service.</td></tr><tr><td><i>guest</i></td><td>Guest.</td></tr></table>	Option	Description	<i>firewall</i>	Firewall.	<i>fsso-service</i>	Fortinet Single Sign-On Service.	<i>rsso</i>	RADIUS based Single Sign-On Service.	<i>guest</i>	Guest.			
	Option	Description												
	<i>firewall</i>	Firewall.												
	<i>fsso-service</i>	Fortinet Single Sign-On Service.												
	<i>rsso</i>	RADIUS based Single Sign-On Service.												
<i>guest</i>	Guest.													
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35											
id	Group ID. Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295											
max-accounts	Maximum number of guest accounts that can be created for this group (0 means unlimited).	integer	Minimum value: 0 0 Maximum value: 1024 **											
member <name>	Names of users, peers, LDAP severs, RADIUS servers or external idp servers to add to the user group. Group member name.	string	Maximum length: 511											
mobile-phone	Enable/disable the guest user mobile phone number field.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.	<i>enable</i>	Enable setting.							
	Option	Description												
	<i>disable</i>	Disable setting.												
<i>enable</i>	Enable setting.													
multiple-guest-add	Enable/disable addition of multiple guests.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.	<i>enable</i>	Enable setting.							
	Option	Description												
	<i>disable</i>	Disable setting.												
<i>enable</i>	Enable setting.													
name	Group name.	string	Maximum length: 35											
password	Guest user password type.	option	-	auto-generate										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto-generate</i>	Automatically generate.		
	<i>specify</i>	Specify.		
	<i>disable</i>	Disable.		
sms-custom-server	SMS server.	string	Maximum length: 35	
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard
	Option	Description		
	<i>fortiguard</i>	Send SMS by FortiGuard.		
	<i>custom</i>	Send SMS by custom server.		
sponsor	Set the action for the sponsor guest user field.	option	-	optional
	Option	Description		
	<i>optional</i>	Optional.		
	<i>mandatory</i>	Mandatory.		
	<i>disabled</i>	Disabled.		
sso-attribute-value	RADIUS attribute value.	string	Maximum length: 511	
user-id	Guest user ID type.	option	-	email
	Option	Description		
	<i>email</i>	Email address.		
	<i>auto-generate</i>	Automatically generate.		
	<i>specify</i>	Specify.		
user-name	Enable/disable the guest user name entry.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable setting.		
	<i>enable</i>	Enable setting.		

** Values may differ between models.

config guest

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
company	Set the action for the company guest user field.	string	Maximum length: 35	
email	Email.	string	Maximum length: 64	
expiration	Expire time.	user	Not Specified	
id	Guest ID.	integer	Minimum value: 0 Maximum value: 4294967295	
mobile-phone	Mobile phone.	string	Maximum length: 35	
name	Guest name.	string	Maximum length: 64	
password	Guest password.	password	Not Specified	
sponsor	Set the action for the sponsor guest user field.	string	Maximum length: 35	
user-id	Guest ID.	string	Maximum length: 64	

config match

Parameter	Description	Type	Size	Default
group-name	Name of matching user or group on remote authentication server or SCIM.	string	Maximum length: 511	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
server-name	Name of remote auth server.	string	Maximum length: 35	

config user krb-keytab

Configure Kerberos keytab entries.

```

config user krb-keytab
  Description: Configure Kerberos keytab entries.
  edit <name>
    set keytab {string}
    set ldap-server <name1>, <name2>, ...
    set pac-data [enable|disable]
    set principal {string}
  next
end

```

config user krb-keytab

Parameter	Description	Type	Size	Default						
keytab	Base64 coded keytab file containing a pre-shared key.	string	Maximum length: 8191							
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79							
name	Kerberos keytab entry name.	string	Maximum length: 35							
pac-data	Enable/disable parsing PAC data in the ticket.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable parsing PAC data in the ticket.</td></tr><tr><td><i>disable</i></td><td>Disable parsing PAC data in the ticket.</td></tr></table>				Option	Description	<i>enable</i>	Enable parsing PAC data in the ticket.	<i>disable</i>	Disable parsing PAC data in the ticket.
Option	Description									
<i>enable</i>	Enable parsing PAC data in the ticket.									
<i>disable</i>	Disable parsing PAC data in the ticket.									
principal	Kerberos service principal. For example, HTTP/myfgt.example.com@example.com.	string	Maximum length: 511							

config user ldap

Configure LDAP server entries.

```

config user ldap
  Description: Configure LDAP server entries.
  edit <name>
    set account-key-cert-field [othername|rfc822name|...]
    set account-key-filter {string}
    set account-key-processing [same|strip]
    set antiphish [enable|disable]
    set ca-cert {string}
    set client-cert {string}
    set client-cert-auth [enable|disable]
    set cnid {string}
    set dn {string}
  next
end

```

```

set group-filter {string}
set group-member-check [user-attr|group-object|...]
set group-object-filter {string}
set group-search-base {string}
set interface {string}
set interface-select-method [auto|sdwan|...]
set member-attr {string}
set obtain-user-info [enable|disable]
set password {password}
set password-attr {string}
set password-expiry-warning [enable|disable]
set password-renewal [enable|disable]
set port {integer}
set search-type {option1}, {option2}, ...
set secondary-server {string}
set secure [disable|starttls|...]
set server {string}
set server-identity-check [enable|disable]
set source-ip {string}
set source-ip-interface {string}
set source-port {integer}
set ssl-min-proto-version [default|SSLv3|...]
set status-ttl {integer}
set tertiary-server {string}
set two-factor [disable|fortitoken-cloud]
set two-factor-authentication [fortitoken|email|...]
set two-factor-filter {string}
set two-factor-notification [email|sms]
set type [simple|anonymous|...]
set user-info-exchange-server {string}
set username {string}
set vrf-select {integer}

next
end

```

config user ldap

Parameter	Description	Type	Size	Default
account-key-cert-field	Define subject identity field in certificate for user access right checking.	option	-	othername
Option	Description			
<i>othername</i>	Other name in SAN.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>rfc822name</i>	RFC822 email address in SAN.		
	<i>dnsname</i>	DNS name in SAN.		
	<i>cn</i>	CN in subject.		
account-key-filter	Account key filter, using the UPN as the search filter.	string	Maximum length: 2047	(&(userPrincipalName=%s)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
account-key-processing	Account key processing operation. The FortiGate will keep either the whole domain or strip the domain from the subject identity.	option	-	same
	Option	Description		
	<i>same</i>	Same as subject identity field.		
	<i>strip</i>	Strip domain string from subject identity field.		
antiphish	Enable/disable AntiPhishing credential backend.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable AntiPhishing credential backend.		
	<i>disable</i>	Disable AntiPhishing credential backend.		
ca-cert	CA certificate name.	string	Maximum length: 79	
client-cert	Client certificate name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
client-cert-auth	Enable/disable using client certificate for TLS authentication.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable using client certificate for TLS authentication.	
	<i>disable</i>		Disable using client certificate for TLS authentication.	
cnid	Common name identifier for the LDAP server. The common name identifier for most LDAP servers is "cn".	string	Maximum length: 20	cn
dn	Distinguished name used to look up entries on the LDAP server.	string	Maximum length: 511	
group-filter	Filter used for group matching.	string	Maximum length: 2047	
group-member-check	Group member checking methods.	option	-	user-attr
	Option		Description	
	<i>user-attr</i>		User attribute checking.	
	<i>group-object</i>		Group object checking.	
	<i>posix-group-object</i>		POSIX group object checking.	
group-object-filter	Filter used for group searching.	string	Maximum length: 2047	(&(objectcategory=group)(member=*))
group-search-base	Search base used for group searching.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63	memberOf								
name	LDAP server entry name.	string	Maximum length: 35									
obtain-user-info	Enable/disable obtaining of user information.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable obtaining of user information.</td></tr><tr><td>disable</td><td>Disable obtaining of user information.</td></tr></table>	Option	Description	enable	Enable obtaining of user information.	disable	Disable obtaining of user information.					
Option	Description											
enable	Enable obtaining of user information.											
disable	Disable obtaining of user information.											
password	Password for initial binding.	password	Not Specified									
password-attr	Name of attribute to get password hash.	string	Maximum length: 35	userPassword								
password-expiry-warning	Enable/disable password expiry warnings.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable password expiry warnings.		
	<i>disable</i>	Disable password expiry warnings.		
password-renewal	Enable/disable online password renewal.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable online password renewal.		
	<i>disable</i>	Disable online password renewal.		
port	Port to be used for communication with the LDAP server (default = 389).	integer	Minimum value: 1 Maximum value: 65535	389
search-type	Search type.	option	-	
	Option	Description		
	<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.		
secondary-server	Secondary LDAP server CN domain name or IP.	string	Maximum length: 63	
secure	Port to be used for authentication.	option	-	disable
	Option	Description		
	<i>disable</i>	No SSL.		
	<i>starttls</i>	Use StartTLS.		
	<i>ldaps</i>	Use LDAPS.		
server	LDAP server CN domain name or IP.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
server-identity-check	Enable/disable LDAP server identity check (verify server domain name/IP address against the server certificate).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server identity check.</td></tr><tr><td><i>disable</i></td><td>Disable server identity check.</td></tr></table>	Option	Description	<i>enable</i>	Enable server identity check.	<i>disable</i>	Disable server identity check.			
Option	Description									
<i>enable</i>	Enable server identity check.									
<i>disable</i>	Disable server identity check.									
source-ip	FortiGate IP address to be used for communication with the LDAP server.	string	Maximum length: 63							
source-ip-interface	Source interface for communication with the LDAP server.	string	Maximum length: 15							
source-port	Source port to be used for communication with the LDAP server.	integer	Minimum value: 0 Maximum value: 65535	0						
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
	<i>TLSv1-3</i>	TLSv1.3.		
status-ttl	Time for which server reachability is cached so that when a server is unreachable, it will not be retried for at least this period of time (0 = cache disabled, default = 300).	integer	Minimum value: 0 Maximum value: 600	300
tertiary-server	Tertiary LDAP server CN domain name or IP.	string	Maximum length: 63	
two-factor	Enable/disable two-factor authentication.	option	-	disable
	Option	Description		
	<i>disable</i>	disable two-factor authentication.		
	<i>fortitoken-cloud</i>	FortiToken Cloud Service.		
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>fortitoken</i>	FortiToken authentication.		
	<i>email</i>	Email one time password.		
	<i>sms</i>	SMS one time password.		
two-factor-filter	Filter used to synchronize users to FortiToken Cloud.	string	Maximum length: 2047	
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	Option	Description		
	<i>email</i>	Email notification for activation code.		
	<i>sms</i>	SMS notification for activation code.		
type	Authentication type for LDAP searches.	option	-	simple
	Option	Description		
	<i>simple</i>	Simple password authentication without search.		
	<i>anonymous</i>	Bind using anonymous user search.		
	<i>regular</i>	Bind using username/password and then search.		
user-info-exchange-server	MS Exchange server from which to fetch user information.	string	Maximum length: 35	
username	Username (full DN) for initial binding.	string	Maximum length: 511	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config user local

Configure local users.

```
config user local
  Description: Configure local users.
  edit <name>
    set auth-concurrent-override [enable|disable]
    set auth-concurrent-value {integer}
    set authtimeout {integer}
    set email-to {string}
    set fortitoken {string}
    set id {integer}
    set ldap-server {string}
    set passwd {password}
    set passwd-policy {string}
    set passwd-time {user}
    set ppk-identity {string}
    set ppk-secret {password-3}
    set qkd-profile {string}
    set radius-server {string}
    set saml-server {string}
    set sms-custom-server {string}
    set sms-phone {string}
    set sms-server [fortiguard|custom]
    set status [enable|disable]
    set tacacs+-server {string}
    set two-factor [disable|fortitoken|...]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set type [password|radius|...]
    set username-sensitivity [disable|enable]
    set workstation {string}
  next
end
```

config user local

Parameter	Description	Type	Size	Default						
auth-concurrent-override	Enable/disable overriding the policy-auth-concurrent under config system global.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auth-concurrent-override.</td></tr><tr><td><i>disable</i></td><td>Disable auth-concurrent-override.</td></tr></table>	Option	Description	<i>enable</i>	Enable auth-concurrent-override.	<i>disable</i>	Disable auth-concurrent-override.			
Option	Description									
<i>enable</i>	Enable auth-concurrent-override.									
<i>disable</i>	Disable auth-concurrent-override.									

Parameter	Description	Type	Size	Default
auth-concurrent-value	Maximum number of concurrent logins permitted from the same user.	integer	Minimum value: 0 Maximum value: 100	0
authtimeout	Time in minutes before the authentication timeout for a user is reached.	integer	Minimum value: 0 Maximum value: 1440	0
email-to	Two-factor recipient's email address.	string	Maximum length: 63	
fortitoken	Two-factor recipient's FortiToken serial number.	string	Maximum length: 16	
id	User ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295	0
ldap-server	Name of LDAP server with which the user must authenticate.	string	Maximum length: 35	
name	Local user name.	string	Maximum length: 64	
passwd	User's password.	password	Not Specified	
passwd-policy	Password policy to apply to this user, as defined in config user password-policy.	string	Maximum length: 35	
passwd-time	Time of the last password update.	user	Not Specified	
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35	
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
qkd-profile	Quantum Key Distribution (QKD) profile.	string	Maximum length: 35	
radius-server	Name of RADIUS server with which the user must authenticate.	string	Maximum length: 35	
saml-server	Name of SAML server with which the user must authenticate.	string	Maximum length: 35	
sms-custom-server	Two-factor recipient's SMS server.	string	Maximum length: 35	
sms-phone	Two-factor recipient's mobile phone number.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default												
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fortiguard</td><td>Send SMS by FortiGuard.</td></tr><tr><td>custom</td><td>Send SMS by custom server.</td></tr></table>	Option	Description	fortiguard	Send SMS by FortiGuard.	custom	Send SMS by custom server.									
Option	Description															
fortiguard	Send SMS by FortiGuard.															
custom	Send SMS by custom server.															
status	Enable/disable allowing the local user to authenticate with the FortiGate unit.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable user.</td></tr><tr><td>disable</td><td>Disable user.</td></tr></table>	Option	Description	enable	Enable user.	disable	Disable user.									
Option	Description															
enable	Enable user.															
disable	Disable user.															
tacacs+-server	Name of TACACS+ server with which the user must authenticate.	string	Maximum length: 35													
two-factor	Enable/disable two-factor authentication.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>disable</td></tr><tr><td>fortitoken</td><td>FortiToken</td></tr><tr><td>fortitoken-cloud</td><td>FortiToken Cloud Service.</td></tr><tr><td>email</td><td>Email authentication code.</td></tr><tr><td>sms</td><td>SMS authentication code.</td></tr></table>	Option	Description	disable	disable	fortitoken	FortiToken	fortitoken-cloud	FortiToken Cloud Service.	email	Email authentication code.	sms	SMS authentication code.			
Option	Description															
disable	disable															
fortitoken	FortiToken															
fortitoken-cloud	FortiToken Cloud Service.															
email	Email authentication code.															
sms	SMS authentication code.															
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fortitoken</td><td>FortiToken authentication.</td></tr><tr><td>email</td><td>Email one time password.</td></tr><tr><td>sms</td><td>SMS one time password.</td></tr></table>	Option	Description	fortitoken	FortiToken authentication.	email	Email one time password.	sms	SMS one time password.							
Option	Description															
fortitoken	FortiToken authentication.															
email	Email one time password.															
sms	SMS one time password.															
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>email</td><td>Email notification for activation code.</td></tr><tr><td>sms</td><td>SMS notification for activation code.</td></tr></table>	Option	Description	email	Email notification for activation code.	sms	SMS notification for activation code.									
Option	Description															
email	Email notification for activation code.															
sms	SMS notification for activation code.															

Parameter	Description	Type	Size	Default
type	Authentication method.	option	-	password
	Option	Description		
	<i>password</i>	Password authentication.		
	<i>radius</i>	RADIUS server authentication.		
	<i>tacacs+</i>	TACACS+ server authentication.		
	<i>ldap</i>	LDAP server authentication.		
	<i>saml</i>	SAML server authentication.		
username-sensitivity	Enable/disable case and accent sensitivity when performing username matching (accents are stripped and case is ignored when disabled).	option	-	enable
	Option	Description		
	<i>disable</i>	Ignore case and accents. Username at prompt not required to match case or accents.		
	<i>enable</i>	Do not ignore case and accents. Username at prompt must be an exact match.		
workstation	Name of the remote user workstation, if you want to limit the user to authenticate only from a particular workstation.	string	Maximum length: 35	

config user nac-policy

Configure NAC policy matching pattern to identify matching NAC devices.

```

config user nac-policy
  Description: Configure NAC policy matching pattern to identify matching NAC devices.
  edit <name>
    set category [device|firewall-user|...]
    set description {string}
    set ems-tag {string}
    set family {string}
    set firewall-address {string}
    set fortivoice-tag {string}
    set host {string}
    set hw-vendor {string}
    set hw-version {string}
    set mac {string}
    set match-period {integer}
    set match-remove [default|link-down]

```



```

set match-type [dynamic|override]
set os {string}
set severity <severity-num1>, <severity-num2>, ...
set src {string}
set ssid-policy {string}
set status [enable|disable]
set sw-version {string}
set switch-fortilink {string}
set switch-group <name1>, <name2>, ...
set switch-mac-policy {string}
set type {string}
set user {string}
set user-group {string}
next
end

```

config user nac-policy

Parameter	Description	Type	Size	Default												
category	Category of NAC policy.	option	-	device												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>device</td><td>Device category.</td></tr><tr><td>firewall-user</td><td>Firewall user category.</td></tr><tr><td>ems-tag</td><td>EMS Tag category.</td></tr><tr><td>fortivoice-tag</td><td>FortiVoice Tag category.</td></tr><tr><td>vulnerability</td><td>Vulnerability category.</td></tr></table>	Option	Description	device	Device category.	firewall-user	Firewall user category.	ems-tag	EMS Tag category.	fortivoice-tag	FortiVoice Tag category.	vulnerability	Vulnerability category.			
	Option	Description														
	device	Device category.														
	firewall-user	Firewall user category.														
	ems-tag	EMS Tag category.														
	fortivoice-tag	FortiVoice Tag category.														
vulnerability	Vulnerability category.															
description	Description for the NAC policy matching pattern.	string	Maximum length: 63													
ems-tag	NAC policy matching EMS tag.	string	Maximum length: 79													
family	NAC policy matching family.	string	Maximum length: 31													
firewall-address *	Dynamic firewall address to associate MAC which match this policy.	string	Maximum length: 79													
fortivoice-tag	NAC policy matching FortiVoice tag.	string	Maximum length: 79													
host	NAC policy matching host.	string	Maximum length: 64													
hw-vendor	NAC policy matching hardware vendor.	string	Maximum length: 15													

Parameter	Description	Type	Size	Default						
hw-version	NAC policy matching hardware version.	string	Maximum length: 15							
mac	NAC policy matching MAC address.	string	Maximum length: 17							
match-period	Number of days the matched devices will be retained (0 - always retain)	integer	Minimum value: 0 Maximum value: 120	0						
match-remove	Options to remove the matched override devices.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Remove the matched override devices based on the match period.</td></tr><tr><td>link-down</td><td>Remove the matched override devices based on switch port link down event.</td></tr></table>				Option	Description	default	Remove the matched override devices based on the match period.	link-down	Remove the matched override devices based on switch port link down event.
Option	Description									
default	Remove the matched override devices based on the match period.									
link-down	Remove the matched override devices based on switch port link down event.									
match-type	Match and retain the devices based on the type.	option	-	dynamic						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dynamic</td><td>Matched devices will be removed on dynamic events like link-down,device-inactivity,switch-offline.</td></tr><tr><td>override</td><td>Matched devices will be retained until the match-period.</td></tr></table>				Option	Description	dynamic	Matched devices will be removed on dynamic events like link-down,device-inactivity,switch-offline.	override	Matched devices will be retained until the match-period.
Option	Description									
dynamic	Matched devices will be removed on dynamic events like link-down,device-inactivity,switch-offline.									
override	Matched devices will be retained until the match-period.									
name	NAC policy name.	string	Maximum length: 63							
os	NAC policy matching operating system.	string	Maximum length: 31							
severity <severity-num>	NAC policy matching devices vulnerability severity lists. Enter multiple severity levels, where 0 = Info, 1 = Low, ..., 4 = Critical	integer	Minimum value: 0 Maximum value: 4							
src	NAC policy matching source.	string	Maximum length: 15							
ssid-policy	SSID policy to be applied on the matched NAC policy.	string	Maximum length: 35							
status	Enable/disable NAC policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NAC policy.</td></tr></table>				Option	Description	enable	Enable NAC policy.		
Option	Description									
enable	Enable NAC policy.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable NAC policy.		
sw-version	NAC policy matching software version.	string	Maximum length: 15	
switch-fortilink *	FortiLink interface for which this NAC policy belongs to.	string	Maximum length: 15	
switch-group <name> *	List of managed FortiSwitch groups on which NAC policy can be applied. Managed FortiSwitch group name from available options.	string	Maximum length: 79	
switch-mac-policy *	Switch MAC policy action to be applied on the matched NAC policy.	string	Maximum length: 63	
type	NAC policy matching type.	string	Maximum length: 15	
user	NAC policy matching user.	string	Maximum length: 64	
user-group	NAC policy matching user group.	string	Maximum length: 35	

* This parameter may not exist in some models.

config user password-policy

Configure user password policy.

```
config user password-policy
  Description: Configure user password policy.
  edit <name>
    set expire-days {integer}
    set expire-status [enable|disable]
    set expired-password-renewal [enable|disable]
    set min-change-characters {integer}
    set min-lower-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-upper-case-letter {integer}
    set minimum-length {integer}
    set reuse-password [enable|disable]
    set reuse-password-limit {integer}
    set warn-days {integer}
  next
end
```

config user password-policy

Parameter	Description	Type	Size	Default						
expire-days	Time in days before the user's password expires.	integer	Minimum value: 0 Maximum value: 999	180						
expire-status	Enable/disable password expiration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Passwords expire after expire-day days.</td></tr><tr><td><i>disable</i></td><td>Passwords do not expire.</td></tr></table>				Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.
Option	Description									
<i>enable</i>	Passwords expire after expire-day days.									
<i>disable</i>	Passwords do not expire.									
expired-password-renewal	Enable/disable renewal of a password that already is expired.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable renewal of a password that already is expired.</td></tr><tr><td><i>disable</i></td><td>Disable renewal of a password that already is expired.</td></tr></table>				Option	Description	<i>enable</i>	Enable renewal of a password that already is expired.	<i>disable</i>	Disable renewal of a password that already is expired.
Option	Description									
<i>enable</i>	Enable renewal of a password that already is expired.									
<i>disable</i>	Disable renewal of a password that already is expired.									
min-change-characters	Minimum number of unique characters in new password which do not exist in old password (0 - 128, default = 0. This attribute overrides reuse-password if both are enabled).	integer	Minimum value: 0 Maximum value: 128	0						
min-lower-case-letter	Minimum number of lowercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128	0						

Parameter	Description	Type	Size	Default						
minimum-length	Minimum password length (8 - 128, default = 8).	integer	Minimum value: 8 Maximum value: 128	8						
name	Password policy name.	string	Maximum length: 35							
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Users are allowed to reuse the same password up to a limit.</td></tr><tr><td>disable</td><td>Users must create a new password.</td></tr></table>				Option	Description	enable	Users are allowed to reuse the same password up to a limit.	disable	Users must create a new password.
Option	Description									
enable	Users are allowed to reuse the same password up to a limit.									
disable	Users must create a new password.									
reuse-password-limit	Number of times passwords can be reused (0 - 20, default = 0. If set to 0, can reuse password an unlimited number of times.).	integer	Minimum value: 0 Maximum value: 20	0						
warn-days	Time in days before a password expiration warning message is displayed to the user upon login.	integer	Minimum value: 0 Maximum value: 30	15						

config user peer

Configure peer users.

```

config user peer
  Description: Configure peer users.
  edit <name>
    set ca {string}
    set cn {string}
    set cn-type [string|email|...]
    set mandatory-ca-verify [enable|disable]
    set mfa-mode [none|password|...]
    set mfa-password {password}
    set mfa-server {string}
    set mfa-username {string}
    set ocsf-override-server {string}
    set passwd {password}
    set subject {string}
    set two-factor [enable|disable]
  next
end

```

config user peer

Parameter	Description	Type	Size	Default												
ca	Name of the CA certificate.	string	Maximum length: 127													
cn	Peer certificate common name.	string	Maximum length: 255													
cn-type	Peer certificate common name type.	option	-	string												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>string</i></td><td>Normal string.</td></tr><tr><td><i>email</i></td><td>Email address.</td></tr><tr><td><i>FQDN</i></td><td>Fully Qualified Domain Name.</td></tr><tr><td><i>ipv4</i></td><td>IPv4 address.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 address.</td></tr></table>	Option	Description	<i>string</i>	Normal string.	<i>email</i>	Email address.	<i>FQDN</i>	Fully Qualified Domain Name.	<i>ipv4</i>	IPv4 address.	<i>ipv6</i>	IPv6 address.			
	Option	Description														
	<i>string</i>	Normal string.														
	<i>email</i>	Email address.														
	<i>FQDN</i>	Fully Qualified Domain Name.														
	<i>ipv4</i>	IPv4 address.														
<i>ipv6</i>	IPv6 address.															
mandatory-ca-verify	Determine what happens to the peer if the CA certificate is not installed. Disable to automatically consider the peer certificate as valid.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
mfa-mode	MFA mode for remote peer authentication/authorization.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>password</i></td><td>Specified username/password.</td></tr><tr><td><i>subject-identity</i></td><td>Subject identity extracted from certificate.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>password</i>	Specified username/password.	<i>subject-identity</i>	Subject identity extracted from certificate.							
	Option	Description														
	<i>none</i>	None.														
	<i>password</i>	Specified username/password.														
<i>subject-identity</i>	Subject identity extracted from certificate.															
mfa-password	Unified password for remote authentication. This field may be left empty when RADIUS authentication is used, in which case the FortiGate will use the RADIUS username as a password.	password	Not Specified													
mfa-server	Name of a remote authenticator. Performs client access right check.	string	Maximum length: 35													
mfa-username	Unified username for remote authentication.	string	Maximum length: 35													

Parameter	Description	Type	Size	Default
name	Peer name.	string	Maximum length: 35	
ocsp-override-server	Online Certificate Status Protocol (OCSP) server for certificate retrieval.	string	Maximum length: 35	
passwd	Peer's password used for two-factor authentication.	password	Not Specified	
subject	Peer certificate name constraints.	string	Maximum length: 255	
two-factor	Enable/disable two-factor authentication, applying certificate and password-based authentication.	option	-	disable
	Option	Description		
	enable	Enable 2-factor authentication.		
	disable	Disable 2-factor authentication.		

config user peergrp

Configure peer groups.

```
config user peergrp
  Description: Configure peer groups.
  edit <name>
    set member <name1>, <name2>, ...
  next
end
```

config user peergrp

Parameter	Description	Type	Size	Default
member <name>	Peer group members. Peer group member name.	string	Maximum length: 35	
name	Peer group name.	string	Maximum length: 35	

config user pop3

POP3 server entry configuration.

```
config user pop3
  Description: POP3 server entry configuration.
  edit <name>
    set port {integer}
    set secure [none|starttls|...]
    set server {string}
    set ssl-min-proto-version [default|SSLv3|...]
  next
end
```

config user pop3

Parameter	Description	Type	Size	Default								
name	POP3 server entry name.	string	Maximum length: 35									
port	POP3 service port number.	integer	Minimum value: 0 Maximum value: 65535	0								
secure	SSL connection.	option	-	starttls								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>None.</td></tr><tr><td>starttls</td><td>Use StartTLS.</td></tr><tr><td>pop3s</td><td>Use POP3 over SSL.</td></tr></table>				Option	Description	none	None.	starttls	Use StartTLS.	pop3s	Use POP3 over SSL.
Option	Description											
none	None.											
starttls	Use StartTLS.											
pop3s	Use POP3 over SSL.											
server	Server domain name or IP address.	string	Maximum length: 63									
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr></table>				Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.
Option	Description											
default	Follow system global setting.											
SSLv3	SSLv3.											
TLSv1	TLSv1.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
	<i>TLSv1-3</i>	TLSv1.3.		

config user quarantine

Configure quarantine support.

```

config user quarantine
  Description: Configure quarantine support.
  set firewall-groups {string}
  set quarantine [enable|disable]
  config targets
    Description: Quarantine entry to hold multiple MACs.
    edit <entry>
      set description {string}
      config macs
        Description: Quarantine MACs.
        edit <mac>
          set description {string}
          set drop [disable|enable]
          set parent {string}
        next
      end
    next
  end
  set traffic-policy {string}
end

```

config user quarantine

Parameter	Description	Type	Size	Default
firewall-groups	Firewall address group which includes all quarantine MAC address.	string	Maximum length: 79	
quarantine	Enable/disable quarantine.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable quarantine.		
	<i>disable</i>	Disable quarantine.		

Parameter	Description	Type	Size	Default
traffic-policy *	Traffic policy for quarantined MACs.	string	Maximum length: 63	

* This parameter may not exist in some models.

config targets

Parameter	Description	Type	Size	Default
description	Description for the quarantine entry.	string	Maximum length: 63	
entry	Quarantine entry name.	string	Maximum length: 63	

config macs

Parameter	Description	Type	Size	Default
description	Description for the quarantine MAC.	string	Maximum length: 63	
drop	Enable/disable dropping of quarantined device traffic.	option	-	disable
	Option	Description		
	disable	Sends quarantined device traffic to FortiGate.		
	enable	Blocks quarantined device traffic to FortiGate.		
mac	Quarantine MAC.	mac-address	Not Specified	00:00:00:00:00:00
parent	Parent entry name. Read-only.	string	Maximum length: 63	

config user radius

Configure RADIUS server entries.

```

config user radius
  Description: Configure RADIUS server entries.
  edit <name>
    set account-key-cert-field [othername|rfc822name|...]
    set account-key-processing [same|strip]
    config accounting-server
      Description: Additional accounting servers.

```

```

    edit <id>
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set port {integer}
        set secret {password}
        set server {string}
        set source-ip {string}
        set status [enable|disable]
        set vrf-select {integer}
    next
end
set acct-all-servers [enable|disable]
set acct-interim-interval {integer}
set all-usergroup [disable|enable]
set auth-type [auto|ms_chap_v2|...]
set ca-cert {string}
set call-station-id-type [legacy|IP|...]
set class <name1>, <name2>, ...
set client-cert {string}
set delimiter [plus|comma]
set group-override-attr-type [filter-Id|class]
set h3c-compatibility [enable|disable]
set interface {string}
set interface-select-method [auto|sdwan|...]
set mac-case [uppercase|lowercase]
set mac-password-delimiter [hyphen|single-hyphen|...]
set mac-username-delimiter [hyphen|single-hyphen|...]
set nas-id {string}
set nas-id-type [legacy|custom|...]
set nas-ip {ipv4-address}
set password-encoding [auto|ISO-8859-1]
set password-renewal [enable|disable]
set radius-coa [enable|disable]
set radius-port {integer}
set require-message-authenticator [enable|disable]
set rso [enable|disable]
set rso-context-timeout {integer}
set rso-endpoint-attribute [User-Name|NAS-IP-Address|...]
set rso-endpoint-block-attribute [User-Name|NAS-IP-Address|...]
set rso-ep-one-ip-only [enable|disable]
set rso-flush-ip-session [enable|disable]
set rso-log-flags {option1}, {option2}, ...
set rso-log-period {integer}
set rso-radius-response [enable|disable]
set rso-radius-server-port {integer}
set rso-secret {password}
set rso-validate-request-secret [enable|disable]
set secondary-secret {password}
set secondary-server {string}
set secret {password}
set server {string}
set server-identity-check [enable|disable]

```

```

set source-ip {string}
set source-ip-interface {string}
set sso-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute-key {string}
set sso-attribute-value-override [enable|disable]
set status-ttl {integer}
set switch-controller-acct-fast-framedip-detect {integer}
set switch-controller-nas-ip-dynamic [enable|disable]
set switch-controller-service-type {option1}, {option2}, ...
set tertiary-secret {password}
set tertiary-server {string}
set timeout {integer}
set tls-min-proto-version [default|SSLv3|...]
set transport-protocol [udp|tcp|...]
set use-management-vdom [enable|disable]
set username-case-sensitive [enable|disable]
set vrf-select {integer}
next
end

```

config user radius

Parameter	Description	Type	Size	Default										
account-key-cert-field	Define subject identity field in certificate for user access right checking.	option	-	othername										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>othername</td><td>Other name in SAN.</td></tr><tr><td>rfc822name</td><td>RFC822 email address in SAN.</td></tr><tr><td>dnsname</td><td>DNS name in SAN.</td></tr><tr><td>cn</td><td>CN in subject.</td></tr></table>	Option	Description	othername	Other name in SAN.	rfc822name	RFC822 email address in SAN.	dnsname	DNS name in SAN.	cn	CN in subject.			
	Option	Description												
	othername	Other name in SAN.												
	rfc822name	RFC822 email address in SAN.												
	dnsname	DNS name in SAN.												
cn	CN in subject.													
account-key-processing	Account key processing operation. The FortiGate will keep either the whole domain or strip the domain from the subject identity.	option	-	same										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>same</td><td>Same as subject identity field.</td></tr><tr><td>strip</td><td>Strip domain string from subject identity field.</td></tr></table>	Option	Description	same	Same as subject identity field.	strip	Strip domain string from subject identity field.							
	Option	Description												
	same	Same as subject identity field.												
strip	Strip domain string from subject identity field.													
acct-all-servers	Enable/disable sending of accounting messages to all configured servers (default = disable).	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Send accounting messages to all configured servers.		
	<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.		
acct-interim-interval	Time in seconds between each accounting interim update message.	integer	Minimum value: 0 60 Maximum value: 86400	
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not automatically include this server in a user group.		
	<i>enable</i>	Include this RADIUS server in every user group.		
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-	auto
	Option	Description		
	<i>auto</i>	Use PAP, MSCHAP_v2, and CHAP (in that order).		
	<i>ms_chap_v2</i>	Microsoft Challenge Handshake Authentication Protocol version 2.		
	<i>ms_chap</i>	Microsoft Challenge Handshake Authentication Protocol.		
	<i>chap</i>	Challenge Handshake Authentication Protocol.		
	<i>pap</i>	Password Authentication Protocol.		
ca-cert	CA of server to trust under TLS.	string	Maximum length: 79	
call-station-id-type	Calling & Called station identifier type configuration (default = legacy), this option is not available for 802.1x authentication.	option	-	legacy
	Option	Description		
	<i>legacy</i>	Calling & Called station identifier is the value previously used by each daemon.		
	<i>IP</i>	Calling & Called station identifier is the value of IP address.		
	<i>MAC</i>	Calling & Called station identifier is the value of MAC address.		
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default								
client-cert	Client certificate to use under TLS.	string	Maximum length: 35									
delimiter	Configure delimiter to be used for separating profile group names in the SSO attribute (default = plus character "+").	option	-	plus								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>plus</i></td><td>Plus character "+".</td></tr><tr><td><i>comma</i></td><td>Comma character ",".</td></tr></table>	Option	Description	<i>plus</i>	Plus character "+".	<i>comma</i>	Comma character ",".					
Option	Description											
<i>plus</i>	Plus character "+".											
<i>comma</i>	Comma character ",".											
group-override-attr-type	RADIUS attribute type to override user group information.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>filter-Id</i></td><td>Filter-Id</td></tr><tr><td><i>class</i></td><td>Class</td></tr></table>	Option	Description	<i>filter-Id</i>	Filter-Id	<i>class</i>	Class					
Option	Description											
<i>filter-Id</i>	Filter-Id											
<i>class</i>	Class											
h3c-compatibility	Enable/disable compatibility with the H3C, a mechanism that performs security checking for authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable H3C compatibility.</td></tr><tr><td><i>disable</i></td><td>Disable H3C compatibility.</td></tr></table>	Option	Description	<i>enable</i>	Enable H3C compatibility.	<i>disable</i>	Disable H3C compatibility.					
Option	Description											
<i>enable</i>	Enable H3C compatibility.											
<i>disable</i>	Disable H3C compatibility.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
mac-case	MAC authentication case (default = lowercase).	option	-	lowercase								

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>uppercase</i></td><td>Use uppercase MAC.</td></tr><tr><td><i>lowercase</i></td><td>Use lowercase MAC.</td></tr></table>				Option	Description	<i>uppercase</i>	Use uppercase MAC.	<i>lowercase</i>	Use lowercase MAC.				
	Option	Description												
	<i>uppercase</i>	Use uppercase MAC.												
<i>lowercase</i>	Use lowercase MAC.													
mac-password-delimiter	MAC authentication password delimiter (default = hyphen).	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hyphen</i></td><td>Use hyphen as delimiter for MAC authentication password.</td></tr><tr><td><i>single-hyphen</i></td><td>Use single hyphen as delimiter for MAC authentication password.</td></tr><tr><td><i>colon</i></td><td>Use colon as delimiter for MAC authentication password.</td></tr><tr><td><i>none</i></td><td>No delimiter for MAC authentication password.</td></tr></table>				Option	Description	<i>hyphen</i>	Use hyphen as delimiter for MAC authentication password.	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC authentication password.	<i>colon</i>	Use colon as delimiter for MAC authentication password.	<i>none</i>	No delimiter for MAC authentication password.
	Option	Description												
	<i>hyphen</i>	Use hyphen as delimiter for MAC authentication password.												
	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC authentication password.												
	<i>colon</i>	Use colon as delimiter for MAC authentication password.												
<i>none</i>	No delimiter for MAC authentication password.													
mac-username-delimiter	MAC authentication username delimiter (default = hyphen).	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hyphen</i></td><td>Use hyphen as delimiter for MAC authentication username.</td></tr><tr><td><i>single-hyphen</i></td><td>Use single hyphen as delimiter for MAC authentication username.</td></tr><tr><td><i>colon</i></td><td>Use colon as delimiter for MAC authentication username.</td></tr><tr><td><i>none</i></td><td>No delimiter for MAC authentication username.</td></tr></table>				Option	Description	<i>hyphen</i>	Use hyphen as delimiter for MAC authentication username.	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC authentication username.	<i>colon</i>	Use colon as delimiter for MAC authentication username.	<i>none</i>	No delimiter for MAC authentication username.
	Option	Description												
	<i>hyphen</i>	Use hyphen as delimiter for MAC authentication username.												
	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC authentication username.												
	<i>colon</i>	Use colon as delimiter for MAC authentication username.												
<i>none</i>	No delimiter for MAC authentication username.													
name	RADIUS server entry name.	string	Maximum length: 35											
nas-id	Custom NAS identifier.	string	Maximum length: 255											
nas-id-type	NAS identifier type configuration (default = legacy).	option	-	legacy										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>legacy</i></td><td>NAS-ID value is the value previously used by each daemon.</td></tr><tr><td><i>custom</i></td><td>NAS-ID value is customized.</td></tr><tr><td><i>hostname</i></td><td>NAS-ID value is hostname or HA group name if applicable.</td></tr></table>				Option	Description	<i>legacy</i>	NAS-ID value is the value previously used by each daemon.	<i>custom</i>	NAS-ID value is customized.	<i>hostname</i>	NAS-ID value is hostname or HA group name if applicable.		
	Option	Description												
	<i>legacy</i>	NAS-ID value is the value previously used by each daemon.												
	<i>custom</i>	NAS-ID value is customized.												
<i>hostname</i>	NAS-ID value is hostname or HA group name if applicable.													
nas-ip	IP address used to communicate with the RADIUS server and used as NAS-IP-Address and Called-Station-ID attributes.	ipv4-address	Not Specified	0.0.0.0										

Parameter	Description	Type	Size	Default						
password-encoding	Password encoding.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Use original password encoding.</td></tr><tr><td>ISO-8859-1</td><td>Use ISO-8859-1 password encoding.</td></tr></table>	Option	Description	auto	Use original password encoding.	ISO-8859-1	Use ISO-8859-1 password encoding.			
Option	Description									
auto	Use original password encoding.									
ISO-8859-1	Use ISO-8859-1 password encoding.									
password-renewal	Enable/disable password renewal.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable password renewal.</td></tr><tr><td>disable</td><td>Disable password renewal.</td></tr></table>	Option	Description	enable	Enable password renewal.	disable	Disable password renewal.			
Option	Description									
enable	Enable password renewal.									
disable	Disable password renewal.									
radius-coa	Enable to allow a mechanism to change the attributes of an authentication, authorization, and accounting session after it is authenticated.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable RADIUS CoA.</td></tr><tr><td>disable</td><td>Disable RADIUS CoA.</td></tr></table>	Option	Description	enable	Enable RADIUS CoA.	disable	Disable RADIUS CoA.			
Option	Description									
enable	Enable RADIUS CoA.									
disable	Disable RADIUS CoA.									
radius-port	RADIUS service port number.	integer	Minimum value: 0 0 Maximum value: 65535							
require-message-authenticator	Require message authenticator in authentication response.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Make the validation of message authenticator mandatory in authentication response.</td></tr><tr><td>disable</td><td>Make the validation of message authenticator optional in authentication response.</td></tr></table>	Option	Description	enable	Make the validation of message authenticator mandatory in authentication response.	disable	Make the validation of message authenticator optional in authentication response.			
Option	Description									
enable	Make the validation of message authenticator mandatory in authentication response.									
disable	Make the validation of message authenticator optional in authentication response.									
rsso	Enable/disable RADIUS based single sign on feature.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable RADIUS based single sign on feature.</td></tr><tr><td>disable</td><td>Disable RADIUS based single sign on feature.</td></tr></table>	Option	Description	enable	Enable RADIUS based single sign on feature.	disable	Disable RADIUS based single sign on feature.			
Option	Description									
enable	Enable RADIUS based single sign on feature.									
disable	Disable RADIUS based single sign on feature.									

Parameter	Description	Type	Size	Default
rsso-context-timeout	Time in seconds before the logged out user is removed from the "user context list" of logged on users.	integer	Minimum value: 0 Maximum value: 4294967295	28800
rsso-endpoint-attribute	RADIUS attributes used to extract the user end point identifier from the RADIUS Start record.	option	-	Calling-Station-Id

Option	Description
<i>User-Name</i>	Use this attribute.
<i>NAS-IP-Address</i>	Use this attribute.
<i>Framed-IP-Address</i>	Use this attribute.
<i>Framed-IP-Netmask</i>	Use this attribute.
<i>Filter-Id</i>	Use this attribute.
<i>Login-IP-Host</i>	Use this attribute.
<i>Reply-Message</i>	Use this attribute.
<i>Callback-Number</i>	Use this attribute.
<i>Callback-Id</i>	Use this attribute.
<i>Framed-Route</i>	Use this attribute.
<i>Framed-IPX-Network</i>	Use this attribute.
<i>Class</i>	Use this attribute.
<i>Called-Station-Id</i>	Use this attribute.
<i>Calling-Station-Id</i>	Use this attribute.
<i>NAS-Identifier</i>	Use this attribute.
<i>Proxy-State</i>	Use this attribute.
<i>Login-LAT-Service</i>	Use this attribute.

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>Login-LAT-Node</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Group</td><td>Use this attribute.</td></tr><tr><td>Framed-AppleTalk-Zone</td><td>Use this attribute.</td></tr><tr><td>Acct-Session-Id</td><td>Use this attribute.</td></tr><tr><td>Acct-Multi-Session-Id</td><td>Use this attribute.</td></tr></table>	Option	Description	Login-LAT-Node	Use this attribute.	Login-LAT-Group	Use this attribute.	Framed-AppleTalk-Zone	Use this attribute.	Acct-Session-Id	Use this attribute.	Acct-Multi-Session-Id	Use this attribute.																			
	Option	Description																														
	Login-LAT-Node	Use this attribute.																														
	Login-LAT-Group	Use this attribute.																														
	Framed-AppleTalk-Zone	Use this attribute.																														
	Acct-Session-Id	Use this attribute.																														
Acct-Multi-Session-Id	Use this attribute.																															
rsso-endpoint-block-attribute	RADIUS attributes used to block a user.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>User-Name</td><td>Use this attribute.</td></tr><tr><td>NAS-IP-Address</td><td>Use this attribute.</td></tr><tr><td>Framed-IP-Address</td><td>Use this attribute.</td></tr><tr><td>Framed-IP-Netmask</td><td>Use this attribute.</td></tr><tr><td>Filter-Id</td><td>Use this attribute.</td></tr><tr><td>Login-IP-Host</td><td>Use this attribute.</td></tr><tr><td>Reply-Message</td><td>Use this attribute.</td></tr><tr><td>Callback-Number</td><td>Use this attribute.</td></tr><tr><td>Callback-Id</td><td>Use this attribute.</td></tr><tr><td>Framed-Route</td><td>Use this attribute.</td></tr><tr><td>Framed-IPX-Network</td><td>Use this attribute.</td></tr><tr><td>Class</td><td>Use this attribute.</td></tr><tr><td>Called-Station-Id</td><td>Use this attribute.</td></tr></table>	Option	Description	User-Name	Use this attribute.	NAS-IP-Address	Use this attribute.	Framed-IP-Address	Use this attribute.	Framed-IP-Netmask	Use this attribute.	Filter-Id	Use this attribute.	Login-IP-Host	Use this attribute.	Reply-Message	Use this attribute.	Callback-Number	Use this attribute.	Callback-Id	Use this attribute.	Framed-Route	Use this attribute.	Framed-IPX-Network	Use this attribute.	Class	Use this attribute.	Called-Station-Id	Use this attribute.			
	Option	Description																														
	User-Name	Use this attribute.																														
	NAS-IP-Address	Use this attribute.																														
	Framed-IP-Address	Use this attribute.																														
	Framed-IP-Netmask	Use this attribute.																														
	Filter-Id	Use this attribute.																														
	Login-IP-Host	Use this attribute.																														
	Reply-Message	Use this attribute.																														
	Callback-Number	Use this attribute.																														
	Callback-Id	Use this attribute.																														
	Framed-Route	Use this attribute.																														
	Framed-IPX-Network	Use this attribute.																														
	Class	Use this attribute.																														
Called-Station-Id	Use this attribute.																															

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>Calling-Station-Id</td><td>Use this attribute.</td></tr><tr><td>NAS-Identifier</td><td>Use this attribute.</td></tr><tr><td>Proxy-State</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Service</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Node</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Group</td><td>Use this attribute.</td></tr><tr><td>Framed-AppleTalk-Zone</td><td>Use this attribute.</td></tr><tr><td>Acct-Session-Id</td><td>Use this attribute.</td></tr><tr><td>Acct-Multi-Session-Id</td><td>Use this attribute.</td></tr></table>	Option	Description	Calling-Station-Id	Use this attribute.	NAS-Identifier	Use this attribute.	Proxy-State	Use this attribute.	Login-LAT-Service	Use this attribute.	Login-LAT-Node	Use this attribute.	Login-LAT-Group	Use this attribute.	Framed-AppleTalk-Zone	Use this attribute.	Acct-Session-Id	Use this attribute.	Acct-Multi-Session-Id	Use this attribute.			
	Option	Description																						
	Calling-Station-Id	Use this attribute.																						
	NAS-Identifier	Use this attribute.																						
	Proxy-State	Use this attribute.																						
	Login-LAT-Service	Use this attribute.																						
	Login-LAT-Node	Use this attribute.																						
	Login-LAT-Group	Use this attribute.																						
	Framed-AppleTalk-Zone	Use this attribute.																						
	Acct-Session-Id	Use this attribute.																						
Acct-Multi-Session-Id	Use this attribute.																							
rsso-ep-one-ip-only	Enable/disable the replacement of old IP addresses with new ones for the same endpoint on RADIUS accounting Start messages.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td></tr><tr><td>disable</td><td>Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td></tr></table>	Option	Description	enable	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.	disable	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																	
	Option	Description																						
	enable	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																						
disable	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																							
rsso-flush-ip-session	Enable/disable flushing user IP sessions on RADIUS accounting Stop messages.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable flush user IP sessions on RADIUS accounting stop.</td></tr><tr><td>disable</td><td>Disable flush user IP sessions on RADIUS accounting stop.</td></tr></table>	Option	Description	enable	Enable flush user IP sessions on RADIUS accounting stop.	disable	Disable flush user IP sessions on RADIUS accounting stop.																	
	Option	Description																						
	enable	Enable flush user IP sessions on RADIUS accounting stop.																						
disable	Disable flush user IP sessions on RADIUS accounting stop.																							

Parameter	Description	Type	Size	Default																
rsso-log-flags	Events to log.	option	-	protocol-error profile-missing accounting-stop-missed accounting-event endpoint-block radiusd-other																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>protocol-error</td><td>Enable this log type.</td></tr><tr><td>profile-missing</td><td>Enable this log type.</td></tr><tr><td>accounting-stop-missed</td><td>Enable this log type.</td></tr><tr><td>accounting-event</td><td>Enable this log type.</td></tr><tr><td>endpoint-block</td><td>Enable this log type.</td></tr><tr><td>radiusd-other</td><td>Enable this log type.</td></tr><tr><td>none</td><td>Disable all logging.</td></tr></table>	Option	Description	protocol-error	Enable this log type.	profile-missing	Enable this log type.	accounting-stop-missed	Enable this log type.	accounting-event	Enable this log type.	endpoint-block	Enable this log type.	radiusd-other	Enable this log type.	none	Disable all logging.			
Option	Description																			
protocol-error	Enable this log type.																			
profile-missing	Enable this log type.																			
accounting-stop-missed	Enable this log type.																			
accounting-event	Enable this log type.																			
endpoint-block	Enable this log type.																			
radiusd-other	Enable this log type.																			
none	Disable all logging.																			
rsso-log-period	Time interval in seconds that group event log messages will be generated for dynamic profile events.	integer	Minimum value: 0 0 Maximum value: 4294967295																	
rsso-radius-response	Enable/disable sending RADIUS response packets after receiving Start and Stop records.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending RADIUS response packets.</td></tr><tr><td>disable</td><td>Disable sending RADIUS response packets.</td></tr></table>	Option	Description	enable	Enable sending RADIUS response packets.	disable	Disable sending RADIUS response packets.													
Option	Description																			
enable	Enable sending RADIUS response packets.																			
disable	Disable sending RADIUS response packets.																			
rsso-radius-server-port	UDP port to listen on for RADIUS Start and Stop records.	integer	Minimum value: 1813 0 Maximum value: 65535																	
rsso-secret	RADIUS secret used by the RADIUS accounting server.	password	Not Specified																	

Parameter	Description	Type	Size	Default								
rsso-validate-request-secret	Enable/disable validating the RADIUS request shared secret in the Start or End record.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable validating RADIUS request shared secret.</td></tr><tr><td><i>disable</i></td><td>Disable validating RADIUS request shared secret.</td></tr></table>	Option	Description	<i>enable</i>	Enable validating RADIUS request shared secret.	<i>disable</i>	Disable validating RADIUS request shared secret.					
Option	Description											
<i>enable</i>	Enable validating RADIUS request shared secret.											
<i>disable</i>	Disable validating RADIUS request shared secret.											
secondary-secret	Secret key to access the secondary server.	password	Not Specified									
secondary-server	Secondary RADIUS CN domain name or IP address.	string	Maximum length: 63									
secret	Pre-shared secret key used to access the primary RADIUS server.	password	Not Specified									
server	Primary RADIUS server CN domain name or IP address.	string	Maximum length: 63									
server-identity-check	Enable/disable RADIUS server identity check (verify server domain name/IP address against the server certificate).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server identity check.</td></tr><tr><td><i>disable</i></td><td>Disable server identity check.</td></tr></table>	Option	Description	<i>enable</i>	Enable server identity check.	<i>disable</i>	Disable server identity check.					
Option	Description											
<i>enable</i>	Enable server identity check.											
<i>disable</i>	Disable server identity check.											
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63									
source-ip-interface	Source interface for communication with the RADIUS server.	string	Maximum length: 15									
sso-attribute	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.	option	-	Class								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>User-Name</i></td><td>Use this attribute.</td></tr><tr><td><i>NAS-IP-Address</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IP-Address</i></td><td>Use this attribute.</td></tr></table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.			
Option	Description											
<i>User-Name</i>	Use this attribute.											
<i>NAS-IP-Address</i>	Use this attribute.											
<i>Framed-IP-Address</i>	Use this attribute.											

Parameter	Description	Type	Size	Default																																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>Framed-IP-Netmask</i></td><td>Use this attribute.</td></tr><tr><td><i>Filter-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-IP-Host</i></td><td>Use this attribute.</td></tr><tr><td><i>Reply-Message</i></td><td>Use this attribute.</td></tr><tr><td><i>Callback-Number</i></td><td>Use this attribute.</td></tr><tr><td><i>Callback-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-Route</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IPX-Network</i></td><td>Use this attribute.</td></tr><tr><td><i>Class</i></td><td>Use this attribute.</td></tr><tr><td><i>Called-Station-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Calling-Station-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>NAS-Identifier</i></td><td>Use this attribute.</td></tr><tr><td><i>Proxy-State</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Service</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Node</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Group</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-AppleTalk-Zone</i></td><td>Use this attribute.</td></tr><tr><td><i>Acct-Session-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Acct-Multi-Session-Id</i></td><td>Use this attribute.</td></tr></table>	Option	Description	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.	<i>Callback-Number</i>	Use this attribute.	<i>Callback-Id</i>	Use this attribute.	<i>Framed-Route</i>	Use this attribute.	<i>Framed-IPX-Network</i>	Use this attribute.	<i>Class</i>	Use this attribute.	<i>Called-Station-Id</i>	Use this attribute.	<i>Calling-Station-Id</i>	Use this attribute.	<i>NAS-Identifier</i>	Use this attribute.	<i>Proxy-State</i>	Use this attribute.	<i>Login-LAT-Service</i>	Use this attribute.	<i>Login-LAT-Node</i>	Use this attribute.	<i>Login-LAT-Group</i>	Use this attribute.	<i>Framed-AppleTalk-Zone</i>	Use this attribute.	<i>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.			
	Option	Description																																										
	<i>Framed-IP-Netmask</i>	Use this attribute.																																										
	<i>Filter-Id</i>	Use this attribute.																																										
	<i>Login-IP-Host</i>	Use this attribute.																																										
	<i>Reply-Message</i>	Use this attribute.																																										
	<i>Callback-Number</i>	Use this attribute.																																										
	<i>Callback-Id</i>	Use this attribute.																																										
	<i>Framed-Route</i>	Use this attribute.																																										
	<i>Framed-IPX-Network</i>	Use this attribute.																																										
	<i>Class</i>	Use this attribute.																																										
	<i>Called-Station-Id</i>	Use this attribute.																																										
	<i>Calling-Station-Id</i>	Use this attribute.																																										
	<i>NAS-Identifier</i>	Use this attribute.																																										
	<i>Proxy-State</i>	Use this attribute.																																										
	<i>Login-LAT-Service</i>	Use this attribute.																																										
	<i>Login-LAT-Node</i>	Use this attribute.																																										
	<i>Login-LAT-Group</i>	Use this attribute.																																										
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.																																										
	<i>Acct-Session-Id</i>	Use this attribute.																																										
<i>Acct-Multi-Session-Id</i>	Use this attribute.																																											
sso-attribute-key	Key prefix for SSO group value in the SSO attribute.	string	Maximum length: 35																																									

Parameter	Description	Type	Size	Default
sso-attribute-value-override	Enable/disable override old attribute value with new value for the same endpoint.	option	-	enable
	Option	Description		
	enable	Enable override old attribute value with new value for the same endpoint.		
	disable	Disable override old attribute value with new value for the same endpoint.		
status-ttl	Time for which server reachability is cached so that when a server is unreachable, it will not be retried for at least this period of time (0 = cache disabled, default = 300).	integer	Minimum value: 300 0 Maximum value: 600	
switch-controller-acct-fast-framedip-detect	Switch controller accounting message Framed-IP detection from DHCP snooping (seconds, default=2).	integer	Minimum value: 2 2 Maximum value: 600	
switch-controller-nas-ip-dynamic *	Enable/Disable switch-controller nas-ip dynamic to dynamically set nas-ip.	option	-	disable
	Option	Description		
	enable	Enable dynamic NAS-IP setting.		
	disable	Disable dynamic NAS-IP setting.		
switch-controller-service-type	RADIUS service type.	option	-	
	Option	Description		
	login	User should be connected to a host.		
	framed	User use Framed Protocol.		
	callback-login	User disconnected and called back.		
	callback-framed	User disconnected and called back, then a Framed Protocol.		
	outbound	User granted access to outgoing devices.		
	administrative	User granted access to the administrative unsigned interface.		
	nas-prompt	User provided a command prompt on the NAS.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>authenticate-only</i></td><td>Authentication requested, and no auth info needs to be returned.</td></tr><tr><td><i>callback-nas-prompt</i></td><td>User disconnected and called back, then provided a command prompt.</td></tr><tr><td><i>call-check</i></td><td>Used by the NAS in an Access-Request packet, Access-Accept to answer the call.</td></tr><tr><td><i>callback-administrative</i></td><td>User disconnected and called back, granted access to the admin unsigned interface.</td></tr></table>	Option	Description	<i>authenticate-only</i>	Authentication requested, and no auth info needs to be returned.	<i>callback-nas-prompt</i>	User disconnected and called back, then provided a command prompt.	<i>call-check</i>	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.	<i>callback-administrative</i>	User disconnected and called back, granted access to the admin unsigned interface.							
	Option	Description																
	<i>authenticate-only</i>	Authentication requested, and no auth info needs to be returned.																
	<i>callback-nas-prompt</i>	User disconnected and called back, then provided a command prompt.																
	<i>call-check</i>	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.																
<i>callback-administrative</i>	User disconnected and called back, granted access to the admin unsigned interface.																	
tertiary-secret	Secret key to access the tertiary server.	password	Not Specified															
tertiary-server	Tertiary RADIUS CN domain name or IP address.	string	Maximum length: 63															
timeout	Time in seconds to retry connecting server.	integer	Minimum value: 5 1 Maximum value: 300															
tls-min-protocol-version	Minimum supported protocol version for TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
	Option	Description																
	<i>default</i>	Follow system global setting.																
	<i>SSLv3</i>	SSLv3.																
	<i>TLSv1</i>	TLSv1.																
	<i>TLSv1-1</i>	TLSv1.1.																
	<i>TLSv1-2</i>	TLSv1.2.																
<i>TLSv1-3</i>	TLSv1.3.																	
transport-protocol	Transport protocol to be used (default = udp).	option	-	udp														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>tls</i></td><td>TLS over TCP.</td></tr></table>	Option	Description	<i>udp</i>	UDP.	<i>tcp</i>	TCP.	<i>tls</i>	TLS over TCP.									
	Option	Description																
	<i>udp</i>	UDP.																
	<i>tcp</i>	TCP.																
<i>tls</i>	TLS over TCP.																	
use-management-vdom	Enable/disable using management VDOM to send requests.	option	-	disable														

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send requests using the management VDOM.</td></tr><tr><td><i>disable</i></td><td>Send requests using the current VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Send requests using the management VDOM.	<i>disable</i>	Send requests using the current VDOM.			
	Option	Description								
	<i>enable</i>	Send requests using the management VDOM.								
<i>disable</i>	Send requests using the current VDOM.									
username-case-sensitive	Enable/disable case sensitive user names.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable username case-sensitive.</td></tr><tr><td><i>disable</i></td><td>Disable username case-sensitive.</td></tr></table>	Option	Description	<i>enable</i>	Enable username case-sensitive.	<i>disable</i>	Disable username case-sensitive.			
	Option	Description								
	<i>enable</i>	Enable username case-sensitive.								
<i>disable</i>	Disable username case-sensitive.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 0 Maximum value: 511	0						

* This parameter may not exist in some models.

config accounting-server

Parameter	Description	Type	Size	Default								
id	ID (0 - 4294967295).	integer	Minimum value: 0 0 Maximum value: 4294967295									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
port	RADIUS accounting port number.	integer	Minimum value: 0 0 Maximum value: 65535									
secret	Secret key.	password	Not Specified									

Parameter	Description	Type	Size	Default						
server	Server CN domain name or IP address.	string	Maximum length: 63							
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63							
status	Status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></table>				Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.
	Option	Description								
	<i>enable</i>	Log to remote syslog server.								
<i>disable</i>	Do not log to remote syslog server.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 0 Maximum value: 511							

config user saml

SAML server entry configuration.

```

config user saml
  Description: SAML server entry configuration.
  edit <name>
    set adfs-claim [enable|disable]
    set cert {string}
    set clock-tolerance {integer}
    set digest-method [sha1|sha256]
    set entity-id {string}
    set group-claim-type [email|given-name|...]
    set group-name {string}
    set idp-cert {string}
    set idp-entity-id {string}
    set idp-single-logout-url {string}
    set idp-single-sign-on-url {string}
    set limit-relaystate [enable|disable]
    set reauth [enable|disable]
    set scim-client {string}
    set scim-group-attr-type [display-name|external-id]
    set single-logout-url {string}
    set single-sign-on-url {string}
    set user-claim-type [email|given-name|...]
    set user-name {string}
  next
end

```

config user saml

Parameter	Description	Type	Size	Default
adfs-claim	Enable/disable ADFS Claim for user/group attribute in assertion statement (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ADFS Claim for user/group attribute in assertion statement.		
	<i>disable</i>	Disable ADFS Claim for user/group attribute in assertion statement.		
cert	Certificate to sign SAML messages.	string	Maximum length: 35	
clock-tolerance	Clock skew tolerance in seconds (0 - 300, default = 15, 0 = no tolerance).	integer	Minimum value: 0 Maximum value: 300	15
digest-method	Digest method algorithm (default = sha1).	option	-	sha1
	Option	Description		
	<i>sha1</i>	Digest Method Algorithm is SHA1.		
	<i>sha256</i>	Digest Method Algorithm is SHA256.		
entity-id	SP entity ID.	string	Maximum length: 255	
group-claim-type	Group claim in assertion statement.	option	-	group
	Option	Description		
	<i>email</i>	E-mail address of the user.		
	<i>given-name</i>	Given name of the user.		
	<i>name</i>	Unique name of the user.		
	<i>upn</i>	User principal name (UPN) of the user.		
	<i>common-name</i>	Common name of the user.		
	<i>email-adfs-1x</i>	E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.		
	<i>group</i>	Group that the user is a member of.		
	<i>upn-adfs-1x</i>	User principal name (UPN) of the user.		

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>role</i></td><td>Role that the user has.</td></tr><tr><td><i>sur-name</i></td><td>Surname of the user</td></tr><tr><td><i>ppid</i></td><td>Private identifier of the user.</td></tr><tr><td><i>name-identifier</i></td><td>SAML name identifier of the user.</td></tr><tr><td><i>authentication-method</i></td><td>Method used to authenticate the user.</td></tr><tr><td><i>deny-only-group-sid</i></td><td>Deny-only group SID of the user.</td></tr><tr><td><i>deny-only-primary-sid</i></td><td>Deny-only primary SID of the user.</td></tr><tr><td><i>deny-only-primary-group-sid</i></td><td>Deny-only primary group SID of the user.</td></tr><tr><td><i>group-sid</i></td><td>Group SID of the user.</td></tr><tr><td><i>primary-group-sid</i></td><td>Primary group SID of the user.</td></tr><tr><td><i>primary-sid</i></td><td>Primary SID of the user.</td></tr><tr><td><i>windows-account-name</i></td><td>Domain account name of the user in the form of <domain>\<user>.</td></tr></table>	Option	Description	<i>role</i>	Role that the user has.	<i>sur-name</i>	Surname of the user	<i>ppid</i>	Private identifier of the user.	<i>name-identifier</i>	SAML name identifier of the user.	<i>authentication-method</i>	Method used to authenticate the user.	<i>deny-only-group-sid</i>	Deny-only group SID of the user.	<i>deny-only-primary-sid</i>	Deny-only primary SID of the user.	<i>deny-only-primary-group-sid</i>	Deny-only primary group SID of the user.	<i>group-sid</i>	Group SID of the user.	<i>primary-group-sid</i>	Primary group SID of the user.	<i>primary-sid</i>	Primary SID of the user.	<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.			
	Option	Description																												
	<i>role</i>	Role that the user has.																												
	<i>sur-name</i>	Surname of the user																												
	<i>ppid</i>	Private identifier of the user.																												
	<i>name-identifier</i>	SAML name identifier of the user.																												
	<i>authentication-method</i>	Method used to authenticate the user.																												
	<i>deny-only-group-sid</i>	Deny-only group SID of the user.																												
	<i>deny-only-primary-sid</i>	Deny-only primary SID of the user.																												
	<i>deny-only-primary-group-sid</i>	Deny-only primary group SID of the user.																												
	<i>group-sid</i>	Group SID of the user.																												
	<i>primary-group-sid</i>	Primary group SID of the user.																												
	<i>primary-sid</i>	Primary SID of the user.																												
<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.																													
group-name	Group name in assertion statement.	string	Maximum length: 255																											
idp-cert	IDP Certificate name.	string	Maximum length: 35																											
idp-entity-id	IDP entity ID.	string	Maximum length: 255																											
idp-single-logout-url	IDP single logout url.	string	Maximum length: 255																											
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255																											
limit-relaystate	Enable/disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	option	-	disable																										

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).</td></tr><tr><td><i>disable</i></td><td>Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).</td></tr></table>	Option	Description	<i>enable</i>	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	<i>disable</i>	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).									
	Option	Description														
	<i>enable</i>	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).														
<i>disable</i>	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).															
name	SAML server entry name.	string	Maximum length: 35													
reauth	Enable/disable signalling of IDP to force user re-authentication (default = disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable signalling of IDP to force user re-authentication.</td></tr><tr><td><i>disable</i></td><td>Disable signalling of IDP to force user re-authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable signalling of IDP to force user re-authentication.	<i>disable</i>	Disable signalling of IDP to force user re-authentication.									
	Option	Description														
	<i>enable</i>	Enable signalling of IDP to force user re-authentication.														
<i>disable</i>	Disable signalling of IDP to force user re-authentication.															
scim-client	SCIM client name.	string	Maximum length: 35													
scim-group-attr-type	Group attribute type used to match SCIM groups (default = display-name).	option	-	display-name												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>display-name</i></td><td>Display name.</td></tr><tr><td><i>external-id</i></td><td>External ID.</td></tr></table>	Option	Description	<i>display-name</i>	Display name.	<i>external-id</i>	External ID.									
	Option	Description														
	<i>display-name</i>	Display name.														
<i>external-id</i>	External ID.															
single-logout-url	SP single logout URL.	string	Maximum length: 255													
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255													
user-claim-type	User name claim in assertion statement.	option	-	upn												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>email</i></td><td>E-mail address of the user.</td></tr><tr><td><i>given-name</i></td><td>Given name of the user.</td></tr><tr><td><i>name</i></td><td>Unique name of the user.</td></tr><tr><td><i>upn</i></td><td>User principal name (UPN) of the user.</td></tr><tr><td><i>common-name</i></td><td>Common name of the user.</td></tr></table>	Option	Description	<i>email</i>	E-mail address of the user.	<i>given-name</i>	Given name of the user.	<i>name</i>	Unique name of the user.	<i>upn</i>	User principal name (UPN) of the user.	<i>common-name</i>	Common name of the user.			
	Option	Description														
	<i>email</i>	E-mail address of the user.														
	<i>given-name</i>	Given name of the user.														
	<i>name</i>	Unique name of the user.														
	<i>upn</i>	User principal name (UPN) of the user.														
<i>common-name</i>	Common name of the user.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>email-adfs-1x</i>	E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.		
	<i>group</i>	Group that the user is a member of.		
	<i>upn-adfs-1x</i>	User principal name (UPN) of the user.		
	<i>role</i>	Role that the user has.		
	<i>sur-name</i>	Surname of the user		
	<i>ppid</i>	Private identifier of the user.		
	<i>name-identifier</i>	SAML name identifier of the user.		
	<i>authentication-method</i>	Method used to authenticate the user.		
	<i>deny-only-group-sid</i>	Deny-only group SID of the user.		
	<i>deny-only-primary-sid</i>	Deny-only primary SID of the user.		
	<i>deny-only-primary-group-sid</i>	Deny-only primary group SID of the user.		
	<i>group-sid</i>	Group SID of the user.		
	<i>primary-group-sid</i>	Primary group SID of the user.		
	<i>primary-sid</i>	Primary SID of the user.		
<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.			
user-name	User name in assertion statement.	string	Maximum length: 255	

config user scim

Configure SCIM client entries.

```

config user scim
  Description: Configure SCIM client entries.
  edit <name>
    set auth-method [token|base]
    set base-url {string}
    set certificate {string}

```

```

    set client-identity-check [enable|disable]
    set id {integer}
    set secret {password}
    set status [enable|disable]
    set token-certificate {string}
next
end

```

config user scim

Parameter	Description	Type	Size	Default						
auth-method	TLS client authentication methods (default = bearer token).	option	-	token						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>token</td><td>Bearer token.</td></tr><tr><td>base</td><td>Base.</td></tr></table>				Option	Description	token	Bearer token.	base	Base.
	Option	Description								
	token	Bearer token.								
base	Base.									
base-url	Server URL to receive SCIM create, read, update, delete (CRUD) requests.	string	Maximum length: 127							
certificate	Certificate for client verification during TLS handshake.	string	Maximum length: 79							
client-identity-check	Enable/disable client identity check.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable client identity check.</td></tr><tr><td>disable</td><td>Disable client identity check.</td></tr></table>				Option	Description	enable	Enable client identity check.	disable	Disable client identity check.
	Option	Description								
	enable	Enable client identity check.								
disable	Disable client identity check.									
id	SCIM client ID.	integer	Minimum value: 0 Maximum value: 4294967295							
name	SCIM client name.	string	Maximum length: 35							
secret	Secret for token verification or base authentication.	password	Not Specified							
status	Enable/disable System for Cross-domain Identity Management (SCIM).	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable System for Cross-domain Identity Management (SCIM).		
	<i>disable</i>	Disable System for Cross-domain Identity Management (SCIM).		
token-certificate	Certificate for token verification.	string	Maximum length: 79	

config user security-exempt-list

Configure security exemption list.

```

config user security-exempt-list
  Description: Configure security exemption list.
  edit <name>
    set description {string}
    config rule
      Description: Configure rules for exempting users from captive portal authentication.
      edit <id>
        set dstaddr <name1>, <name2>, ...
        set service <name1>, <name2>, ...
        set srcaddr <name1>, <name2>, ...
      next
    next
  end
next
end

```

config user security-exempt-list

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
name	Name of the exempt list.	string	Maximum length: 35	

config rule

Parameter	Description	Type	Size	Default
dstaddr <name>	Destination addresses or address groups. Address or group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
service <name>	Destination services. Service name.	string	Maximum length: 79	
srcaddr <name>	Source addresses or address groups. Address or group name.	string	Maximum length: 79	

config user setting

Configure user authentication setting.

```

config user setting
    Description: Configure user authentication setting.
    set auth-blackout-time {integer}
    set auth-ca-cert {string}
    set auth-cert {string}
    set auth-http-basic [enable|disable]
    set auth-invalid-max {integer}
    set auth-lockout-duration {integer}
    set auth-lockout-threshold {integer}
    set auth-on-demand [always|implicitly]
    set auth-portal-timeout {integer}
    config auth-ports
        Description: Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and
        TELNET.
        edit <id>
            set port {integer}
            set type [http|https|...]
        next
    end
    set auth-secure-http [enable|disable]
    set auth-src-mac [enable|disable]
    set auth-ssl-allow-renegotiation [enable|disable]
    set auth-ssl-max-proto-version [ssl3|tlsv1|...]
    set auth-ssl-min-proto-version [default|SSLv3|...]
    set auth-ssl-sigalgs [no-rsa-pss|all]
    set auth-timeout {integer}
    set auth-timeout-type [idle-timeout|hard-timeout|...]
    set auth-type {option1}, {option2}, ...
    set cors [disable|enable]
    set cors-allowed-origins <name1>, <name2>, ...
    set default-user-password-policy {string}
    set per-policy-disclaimer [enable|disable]

```

```

set radius-ses-timeout-act [hard-timeout|ignore-timeout]
end

```

config user setting

Parameter	Description	Type	Size	Default						
auth-blackout-time	Time in seconds an IP address is denied access after failing to authenticate five times within one minute.	integer	Minimum value: 0 0 Maximum value: 3600							
auth-ca-cert	HTTPS CA certificate for policy authentication.	string	Maximum length: 35							
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35							
auth-http-basic	Enable/disable use of HTTP basic authentication for identity-based firewall policies.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 5 1 Maximum value: 100							
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 0 Maximum value: 4294967295							
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 3 1 Maximum value: 10							
auth-on-demand	Always/implicitly trigger firewall authentication on demand.	option	-	implicitly						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>always</i></td><td>Always trigger firewall authentication on demand.</td></tr><tr><td><i>implicitly</i></td><td>Implicitly trigger firewall authentication on demand.</td></tr></table>	Option	Description	<i>always</i>	Always trigger firewall authentication on demand.	<i>implicitly</i>	Implicitly trigger firewall authentication on demand.			
Option	Description									
<i>always</i>	Always trigger firewall authentication on demand.									
<i>implicitly</i>	Implicitly trigger firewall authentication on demand.									
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate (1 - 30 min, default 3 min).	integer	Minimum value: 3 1 Maximum value: 30							

Parameter	Description	Type	Size	Default												
auth-secure-http	Enable/disable redirecting HTTP user authentication to more secure HTTPS.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
auth-src-mac	Enable/disable source MAC for user identity.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source MAC for user identity.</td></tr><tr><td><i>disable</i></td><td>Disable source MAC for user identity.</td></tr></table>	Option	Description	<i>enable</i>	Enable source MAC for user identity.	<i>disable</i>	Disable source MAC for user identity.									
Option	Description															
<i>enable</i>	Enable source MAC for user identity.															
<i>disable</i>	Disable source MAC for user identity.															
auth-ssl-allow-renegotiation	Allow/forbid SSL re-negotiation for HTTPS authentication.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow SSL re-negotiation.</td></tr><tr><td><i>disable</i></td><td>Forbid SSL re-negotiation.</td></tr></table>	Option	Description	<i>enable</i>	Allow SSL re-negotiation.	<i>disable</i>	Forbid SSL re-negotiation.									
Option	Description															
<i>enable</i>	Allow SSL re-negotiation.															
<i>disable</i>	Forbid SSL re-negotiation.															
auth-ssl-max-proto-version	Maximum supported protocol version for SSL/TLS connections (default is no limit).	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl3</i></td><td>SSLv3.</td></tr><tr><td><i>tlsv1</i></td><td>TLSv1.</td></tr><tr><td><i>tlsv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>tlsv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>tlsv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>ssl3</i>	SSLv3.	<i>tlsv1</i>	TLSv1.	<i>tlsv1-1</i>	TLSv1.1.	<i>tlsv1-2</i>	TLSv1.2.	<i>tlsv1-3</i>	TLSv1.3.			
Option	Description															
<i>ssl3</i>	SSLv3.															
<i>tlsv1</i>	TLSv1.															
<i>tlsv1-1</i>	TLSv1.1.															
<i>tlsv1-2</i>	TLSv1.2.															
<i>tlsv1-3</i>	TLSv1.3.															
auth-ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.							
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
	<i>TLSv1-3</i>	TLSv1.3.		
auth-ssl-sigalgs	Set signature algorithms related to HTTPS authentication (affects TLS version <= 1.2 only, default is to enable all).	option	-	all
	Option	Description		
	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for HTTPS authentication.		
	<i>all</i>	Enable all supported signature algorithms for HTTPS authentication.		
auth-timeout	Time in minutes before the firewall user authentication timeout requires the user to re-authenticate.	integer	Minimum value: 5 1 Maximum value: 1440	
auth-timeout-type	Control if authenticated users have to login again after a hard timeout, after an idle timeout, or after a session timeout.	option	-	idle-timeout
	Option	Description		
	<i>idle-timeout</i>	Idle timeout.		
	<i>hard-timeout</i>	Hard timeout.		
	<i>new-session</i>	New session timeout.		
auth-type	Supported firewall policy authentication protocols/methods.	option	-	http https ftp telnet
	Option	Description		
	<i>http</i>	Allow HTTP authentication.		
	<i>https</i>	Allow HTTPS authentication.		
	<i>ftp</i>	Allow FTP authentication.		
	<i>telnet</i>	Allow TELNET authentication.		
cors	Enable/disable allowed origins white list for CORS.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable allowed origins white list for CORS.		
	<i>enable</i>	Enable allowed origins white list for CORS.		
cors-allowed-origins <name>	Allowed origins white list for CORS. Allowed origin for CORS.	string	Maximum length: 79	
default-user-password-policy	Default password policy to apply to all local users unless otherwise specified, as defined in config user password-policy.	string	Maximum length: 35	
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable per policy disclaimer.		
	<i>disable</i>	Disable per policy disclaimer.		
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-	hard-timeout
	Option	Description		
	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.		
	<i>ignore-timeout</i>	Ignore session timeout from RADIUS.		

config auth-ports

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535	1024						
type	Service type.	option	-	http						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP service.</td></tr><tr><td>https</td><td>HTTPS service.</td></tr></table>				Option	Description	http	HTTP service.	https	HTTPS service.
Option	Description									
http	HTTP service.									
https	HTTPS service.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ftp</i>	FTP service.		
	<i>telnet</i>	TELNET service.		

config user tacacs+

Configure TACACS+ server entries.

```

config user tacacs+
  Description: Configure TACACS+ server entries.
  edit <name>
    set authen-type [mschap|chap|...]
    set authorization [enable|disable]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set key {password}
    set port {integer}
    set secondary-key {password}
    set secondary-server {string}
    set server {string}
    set source-ip {string}
    set status-ttl {integer}
    set tertiary-key {password}
    set tertiary-server {string}
    set vrf-select {integer}
  next
end

```

config user tacacs+

Parameter	Description	Type	Size	Default
authen-type	Allowed authentication protocols/methods.	option	-	auto
	Option	Description		
	<i>mschap</i>	MSCHAP.		
	<i>chap</i>	CHAP.		
	<i>pap</i>	PAP.		
	<i>ascii</i>	ASCII.		
	<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).		

Parameter	Description	Type	Size	Default								
authorization	Enable/disable TACACS+ authorization.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ authorization.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ authorization.	<i>disable</i>	Disable TACACS+ authorization.					
Option	Description											
<i>enable</i>	Enable TACACS+ authorization.											
<i>disable</i>	Disable TACACS+ authorization.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
key	Key to access the primary server.	password	Not Specified									
name	TACACS+ server entry name.	string	Maximum length: 35									
port	Port number of the TACACS+ server.	integer	Minimum value: 1 Maximum value: 65535	49								
secondary-key	Key to access the secondary server.	password	Not Specified									
secondary-server	Secondary TACACS+ server CN domain name or IP address.	string	Maximum length: 63									
server	Primary TACACS+ server CN domain name or IP address.	string	Maximum length: 63									
source-ip	Source IP address for communications to TACACS+ server.	string	Maximum length: 63									
status-ttl	Time for which server reachability is cached so that when a server is unreachable, it will not be retried for at least this period of time (0 = cache disabled, default = 300).	integer	Minimum value: 0 Maximum value: 600	300								
tertiary-key	Key to access the tertiary server.	password	Not Specified									

Parameter	Description	Type	Size	Default
tertiary-server	Tertiary TACACS+ server CN domain name or IP address.	string	Maximum length: 63	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

videofilter

This section includes syntax for the following commands:

- [config videofilter keyword on page 2089](#)
- [config videofilter profile on page 2090](#)
- [config videofilter youtube-key on page 2093](#)

config videofilter keyword

Configure video filter keywords.

```
config videofilter keyword
  Description: Configure video filter keywords.
  edit <id>
    set comment {var-string}
    set match [or|and]
    set name {string}
    config word
      Description: List of keywords.
      edit <name>
        set comment {var-string}
        set pattern-type [wildcard|regex]
        set status [enable|disable]
      next
    end
  next
end
```

config videofilter keyword

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
match	Keyword matching logic.	option	-	or

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>or</i>	Match any keyword.		
	<i>and</i>	Match all keywords.		
name	Name.	string	Maximum length: 35	

config word

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Name.	string	Maximum length: 79	
pattern-type	Pattern type.	option	-	wildcard
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regex</i>	Perl regular expression.		
status	Enable(consider)/disable(ignore) this keyword.	option	-	enable
	Option	Description		
	<i>enable</i>	Consider this keyword.		
	<i>disable</i>	Ignore this keyword.		

config videofilter profile

Configure VideoFilter profile.

```

config videofilter profile
  Description: Configure VideoFilter profile.
  edit <name>
    set comment {var-string}
    set dailymotion [enable|disable]
    config filters
      Description: YouTube filter entries.
      edit <id>
        set action [allow|monitor|...]
        set category {string}

```

```

        set channel {string}
        set comment {var-string}
        set keyword {integer}
        set log [enable|disable]
        set type [category|channel|...]
    next
end
set replacemsg-group {string}
set vimeo [enable|disable]
set youtube [enable|disable]
next
end

```

config videofilter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
dailymotion	Enable/disable Dailymotion video source.	option	-	enable
	Option	Description		
	enable	Enable Dailymotion source.		
	disable	Disable Dailymotion source.		
name	Name.	string	Maximum length: 47	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
vimeo	Enable/disable Vimeo video source.	option	-	enable
	Option	Description		
	enable	Enable Vimeo source.		
	disable	Disable Vimeo source.		
youtube	Enable/disable YouTube video source.	option	-	enable
	Option	Description		
	enable	Enable YouTube source.		
	disable	Disable YouTube source.		

config filters

Parameter	Description	Type	Size	Default										
action	Video filter action.	option	-	monitor										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow videos to be accessed.</td></tr><tr><td><i>monitor</i></td><td>Monitor videos.</td></tr><tr><td><i>block</i></td><td>Block videos.</td></tr></table>	Option	Description	<i>allow</i>	Allow videos to be accessed.	<i>monitor</i>	Monitor videos.	<i>block</i>	Block videos.					
Option	Description													
<i>allow</i>	Allow videos to be accessed.													
<i>monitor</i>	Monitor videos.													
<i>block</i>	Block videos.													
category	FortiGuard category ID.	string	Maximum length: 7											
channel	Channel ID.	string	Maximum length: 255											
comment	Comment.	var-string	Maximum length: 255											
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295											
keyword	Video filter keyword ID.	integer	Minimum value: 0 0 Maximum value: 4294967295											
log	Enable/disable logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.							
Option	Description													
<i>enable</i>	Enable logging.													
<i>disable</i>	Disable logging.													
type	Filter type.	option	-	category										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>category</i></td><td>Filter videos by FortiGuard category.</td></tr><tr><td><i>channel</i></td><td>Filter videos by channel ID.</td></tr><tr><td><i>title</i></td><td>Filter videos by title.</td></tr><tr><td><i>description</i></td><td>Filter videos by description.</td></tr></table>	Option	Description	<i>category</i>	Filter videos by FortiGuard category.	<i>channel</i>	Filter videos by channel ID.	<i>title</i>	Filter videos by title.	<i>description</i>	Filter videos by description.			
Option	Description													
<i>category</i>	Filter videos by FortiGuard category.													
<i>channel</i>	Filter videos by channel ID.													
<i>title</i>	Filter videos by title.													
<i>description</i>	Filter videos by description.													

config videofilter youtube-key

Configure YouTube API keys.

```
config videofilter youtube-key
  Description: Configure YouTube API keys.
  edit <id>
    set key {string}
  next
end
```

config videofilter youtube-key

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
key	Key.	string	Maximum length: 47	

virtual-patch

This section includes syntax for the following commands:

- [config virtual-patch profile on page 2094](#)

config virtual-patch profile

Configure virtual-patch profile.

```
config virtual-patch profile
  Description: Configure virtual-patch profile.
  edit <name>
    set action [pass|block]
    set comment {var-string}
    config exemption
      Description: Exempt devices or rules.
      edit <id>
        set device <mac1>, <mac2>, ...
        set rule <id1>, <id2>, ...
        set status [enable|disable]
      next
    end
    set log [enable|disable]
    set severity {option1}, {option2}, ...
  next
end
```

config virtual-patch profile

Parameter	Description	Type	Size	Default
action	Action (pass/block).	option	-	block
	Option	Description		
	<i>pass</i>	Allows session that match the profile.		
	<i>block</i>	Blocks sessions that match the profile.		
comment	Comment.	var-string	Maximum length: 255	
log	Enable/disable logging of detection.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		
name	Profile name.	string	Maximum length: 47	
severity	Relative severity of the signature (low, medium, high, critical).	option	-	info low medium high critical
	Option	Description		
	<i>info</i>	info		
	<i>low</i>	low		
	<i>medium</i>	medium		
	<i>high</i>	high		
	<i>critical</i>	critical		

config exemption

Parameter	Description	Type	Size	Default						
device <mac>	Device MAC addresses. Device MAC address.	mac-address	Not Specified							
id	IDs.	integer	Minimum value: 0 Maximum value: 4294967295	0						
rule <id>	Patch signature rule IDs. Rule IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
status	Enable/disable exemption.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable exemption.</td></tr><tr><td>disable</td><td>Disable exemption.</td></tr></table>				Option	Description	enable	Enable exemption.	disable	Disable exemption.
Option	Description									
enable	Enable exemption.									
disable	Disable exemption.									

voip

This section includes syntax for the following commands:

- [config voip profile on page 2096](#)

config voip profile

Configure VoIP profiles.

```
config voip profile
  Description: Configure VoIP profiles.
  edit <name>
    set comment {var-string}
    set feature-set [ips|voipd]
    config msrp
      Description: MSRP.
      set log-violations [disable|enable]
      set max-msg-size {integer}
      set max-msg-size-action [pass|block|...]
      set status [disable|enable]
    end
    config sccp
      Description: SCCP.
      set block-mcast [disable|enable]
      set log-call-summary [disable|enable]
      set log-violations [disable|enable]
      set max-calls {integer}
      set status [disable|enable]
      set verify-header [disable|enable]
    end
    config sip
      Description: SIP.
      set ack-rate {integer}
      set ack-rate-track [none|src-ip|...]
      set block-ack [disable|enable]
      set block-bye [disable|enable]
      set block-cancel [disable|enable]
      set block-geo-red-options [disable|enable]
      set block-info [disable|enable]
      set block-invite [disable|enable]
      set block-long-lines [disable|enable]
      set block-message [disable|enable]
      set block-notify [disable|enable]
      set block-options [disable|enable]
      set block-prack [disable|enable]
```



```
set block-publish [disable|enable]
set block-refer [disable|enable]
set block-register [disable|enable]
set block-subscribe [disable|enable]
set block-unknown [disable|enable]
set block-update [disable|enable]
set bye-rate {integer}
set bye-rate-track [none|src-ip|...]
set call-id-regex {var-string}
set call-keepalive {integer}
set cancel-rate {integer}
set cancel-rate-track [none|src-ip|...]
set contact-fixup [disable|enable]
set content-type-regex {var-string}
set hnt-restrict-source-ip [disable|enable]
set hosted-nat-traversal [disable|enable]
set info-rate {integer}
set info-rate-track [none|src-ip|...]
set invite-rate {integer}
set invite-rate-track [none|src-ip|...]
set ips-rtp [disable|enable]
set log-call-summary [disable|enable]
set log-violations [disable|enable]
set malformed-header-allow [discard|pass|...]
set malformed-header-call-id [discard|pass|...]
set malformed-header-contact [discard|pass|...]
set malformed-header-content-length [discard|pass|...]
set malformed-header-content-type [discard|pass|...]
set malformed-header-cseq [discard|pass|...]
set malformed-header-expires [discard|pass|...]
set malformed-header-from [discard|pass|...]
set malformed-header-max-forwards [discard|pass|...]
set malformed-header-no-proxy-require [discard|pass|...]
set malformed-header-no-require [discard|pass|...]
set malformed-header-p-asserted-identity [discard|pass|...]
set malformed-header-rack [discard|pass|...]
set malformed-header-record-route [discard|pass|...]
set malformed-header-route [discard|pass|...]
set malformed-header-rseq [discard|pass|...]
set malformed-header-sdp-a [discard|pass|...]
set malformed-header-sdp-b [discard|pass|...]
set malformed-header-sdp-c [discard|pass|...]
set malformed-header-sdp-i [discard|pass|...]
set malformed-header-sdp-k [discard|pass|...]
set malformed-header-sdp-m [discard|pass|...]
set malformed-header-sdp-o [discard|pass|...]
set malformed-header-sdp-r [discard|pass|...]
set malformed-header-sdp-s [discard|pass|...]
set malformed-header-sdp-t [discard|pass|...]
set malformed-header-sdp-v [discard|pass|...]
set malformed-header-sdp-z [discard|pass|...]
set malformed-header-to [discard|pass|...]
```

```

set malformed-header-via [discard|pass|...]
set malformed-request-line [discard|pass|...]
set max-body-length {integer}
set max-dialogs {integer}
set max-idle-dialogs {integer}
set max-line-length {integer}
set message-rate {integer}
set message-rate-track [none|src-ip|...]
set nat-port-range {user}
set nat-trace [disable|enable]
set no-sdp-fixup [disable|enable]
set notify-rate {integer}
set notify-rate-track [none|src-ip|...]
set open-contact-pinhole [disable|enable]
set open-record-route-pinhole [disable|enable]
set open-register-pinhole [disable|enable]
set open-via-pinhole [disable|enable]
set options-rate {integer}
set options-rate-track [none|src-ip|...]
set prack-rate {integer}
set prack-rate-track [none|src-ip|...]
set preserve-override [disable|enable]
set provisional-invite-expiry-time {integer}
set publish-rate {integer}
set publish-rate-track [none|src-ip|...]
set refer-rate {integer}
set refer-rate-track [none|src-ip|...]
set register-contact-trace [disable|enable]
set register-rate {integer}
set register-rate-track [none|src-ip|...]
set rfc2543-branch [disable|enable]
set rtp [disable|enable]
set ssl-algorithm [high|medium|...]
set ssl-auth-client {string}
set ssl-auth-server {string}
set ssl-client-certificate {string}
set ssl-client-renegotiation [allow|deny|...]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-mode [off|full]
set ssl-pfs [require|deny|...]
set ssl-send-empty-frags [enable|disable]
set ssl-server-certificate {string}
set status [disable|enable]
set strict-register [disable|enable]
set subscribe-rate {integer}
set subscribe-rate-track [none|src-ip|...]
set unknown-header [discard|pass|...]
set update-rate {integer}
set update-rate-track [none|src-ip|...]
end
next

```

end

config voip profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
feature-set	IPS or voipd (SIP-ALG) inspection feature set.	option	-	voipd
	Option Description			
	ips	IPS Engine feature set for ips-voip-filter.		
	voipd	SIP ALG feature set for voip-profile.		
name	Profile name.	string	Maximum length: 47	

config msrp

Parameter	Description	Type	Size	Default
log-violations	Enable/disable logging of MSRP violations.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-msg-size	Maximum allowable MSRP message size (1-65535).	integer	Minimum value: 0 Maximum value: 65535	0
max-msg-size-action	Action for violation of max-msg-size.	option	-	pass
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
	<i>monitor</i>	Pass and log matching traffic.		
status	Enable/disable MSRP.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		

config sccp

Parameter	Description	Type	Size	Default
block-mcast	Enable/disable block multicast RTP connections.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-call-summary	Enable/disable log summary of SCCP calls.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-violations	Enable/disable logging of SCCP violations.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-calls	Maximum calls per minute per SCCP client (max 65535).	integer	Minimum value: 0 Maximum value: 65535	0
status	Enable/disable SCCP.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
verify-header	Enable/disable verify SCCP header content.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		

config sip

Parameter	Description	Type	Size	Default
ack-rate	ACK request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	0
ack-rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
block-ack	Enable/disable block ACK requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-bye	Enable/disable block BYE requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-cancel	Enable/disable block CANCEL requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-geo-red-options	Enable/disable block OPTIONS requests, but OPTIONS requests still notify for redundancy.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-info	Enable/disable block INFO requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-invite	Enable/disable block INVITE requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-long-lines	Enable/disable block requests with headers exceeding max-line-length.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-message	Enable/disable block MESSAGE requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-notify	Enable/disable block NOTIFY requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-options	Enable/disable block OPTIONS requests and no OPTIONS as notifying message for redundancy either.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-prack	Enable/disable block prack requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-publish	Enable/disable block PUBLISH requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-refer	Enable/disable block REFER requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-register	Enable/disable block REGISTER requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-subscribe	Enable/disable block SUBSCRIBE requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-unknown	Block unrecognized SIP requests (enabled by default).	option	-	enable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.					
	Option	Description										
	<i>disable</i>	Disable status.										
<i>enable</i>	Enable status.											
block-update	Enable/disable block UPDATE requests.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.					
	Option	Description										
	<i>disable</i>	Disable status.										
<i>enable</i>	Enable status.											
bye-rate	BYE request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	0								
bye-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
	Option	Description										
	<i>none</i>	None.										
	<i>src-ip</i>	Source IP.										
<i>dest-ip</i>	Destination IP.											
call-id-regex	Validate PCRE regular expression for Call-Id header value.	var-string	Maximum length: 511									
call-keepalive	Continue tracking calls with no RTP for this many minutes.	integer	Minimum value: 0 0 Maximum value: 10080	0								
cancel-rate	CANCEL request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	0								
cancel-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
	Option	Description										
	<i>none</i>	None.										
	<i>src-ip</i>	Source IP.										
<i>dest-ip</i>	Destination IP.											

Parameter	Description	Type	Size	Default
contact-fixup	Fixup contact anyway even if contact's IP:port doesn't match session's IP:port.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
content-type-regex	Validate PCRE regular expression for Content-Type header value.	var-string	Maximum length: 511	
hnt-restrict-source-ip	Enable/disable restrict RTP source IP to be the same as SIP source IP when HNT is enabled.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
hosted-nat-traversal	Hosted NAT Traversal (HNT).	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
info-rate	INFO request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	
info-rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
invite-rate	INVITE request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	
invite-rate-track	Track the packet protocol field.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
ips-rtp	Enable/disable allow IPS on RTP.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-call-summary	Enable/disable logging of SIP call summary.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-violations	Enable/disable logging of SIP violations.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
malformed-header-allow	Action for malformed Allow header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-call-id	Action for malformed Call-ID header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		

Parameter	Description	Type	Size	Default								
malformed-header-contact	Action for malformed Contact header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-content-length	Action for malformed Content-Length header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-content-type	Action for malformed Content-Type header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-cseq	Action for malformed CSeq header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-expires	Action for malformed Expires header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.					
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>respond</i>	Respond with error code.		
malformed-header-from	Action for malformed From header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-max-forwards	Action for malformed Max-Forwards header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-no-proxy-require	Action for malformed SIP messages without Proxy-Require header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-no-require	Action for malformed SIP messages without Require header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		

Parameter	Description	Type	Size	Default
malformed-header-p-asserted-identity	Action for malformed P-Asserted-Identity header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-rack	Action for malformed RACK header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-record-route	Action for malformed Record-Route header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-route	Action for malformed Route header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-rseq	Action for malformed RSeq header.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-a	Action for malformed SDP a line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-b	Action for malformed SDP b line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-c	Action for malformed SDP c line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-i	Action for malformed SDP i line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-k	Action for malformed SDP k line.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-m	Action for malformed SDP m line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-o	Action for malformed SDP o line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-r	Action for malformed SDP r line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-s	Action for malformed SDP s line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-t	Action for malformed SDP t line.	option	-	pass

Parameter	Description	Type	Size	Default
	Option Description			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-v	Action for malformed SDP v line.	option	-	pass
	Option Description			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-z	Action for malformed SDP z line.	option	-	pass
	Option Description			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-to	Action for malformed To header.	option	-	pass
	Option Description			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-via	Action for malformed VIA header.	option	-	pass
	Option Description			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-request-line	Action for malformed request line.	option	-	pass

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
	Option	Description										
	<i>discard</i>	Discard malformed messages.										
	<i>pass</i>	Bypass malformed messages.										
<i>respond</i>	Respond with error code.											
max-body-length	Maximum SIP message body length (0 meaning no limit).	integer	Minimum value: 0 0 Maximum value: 4294967295									
max-dialogs	Maximum number of concurrent calls/dialogs (per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295									
max-idle-dialogs	Maximum number established but idle dialogs to retain (per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295									
max-line-length	Maximum SIP header line length (78-4096).	integer	Minimum value: 998 78 Maximum value: 4096									
message-rate	MESSAGE request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295									
message-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
	Option	Description										
	<i>none</i>	None.										
	<i>src-ip</i>	Source IP.										
<i>dest-ip</i>	Destination IP.											
nat-port-range	RTP NAT port range.	user	Not Specified	5117-65533								
nat-trace	Enable/disable preservation of original IP in SDP i line.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.							
	Option	Description										
<i>disable</i>	Disable status.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
no-sdp-fixup	Enable/disable no SDP fix-up.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
notify-rate	NOTIFY request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	0
notify-rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
open-contact-pinhole	Enable/disable open pinhole for non-REGISTER Contact port.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
open-record-route-pinhole	Enable/disable open pinhole for Record-Route port.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
open-register-pinhole	Enable/disable open pinhole for REGISTER Contact port.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable status.		
open-via-pinhole	Enable/disable open pinhole for Via port.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
options-rate	OPTIONS request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	0
options-rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
prack-rate	PRACK request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	0
prack-rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
preserve-override	Override i line to preserve original IPs (default: append).	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		

Parameter	Description	Type	Size	Default								
provisional-invite-expiry-time	Expiry time (10-3600, in seconds) for provisional INVITE.	integer	Minimum value: 10 Maximum value: 3600	210								
publish-rate	PUBLISH request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
publish-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>				Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.
	Option	Description										
	<i>none</i>	None.										
	<i>src-ip</i>	Source IP.										
<i>dest-ip</i>	Destination IP.											
refer-rate	REFER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
refer-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>				Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.
	Option	Description										
	<i>none</i>	None.										
	<i>src-ip</i>	Source IP.										
<i>dest-ip</i>	Destination IP.											
register-contact-trace	Enable/disable trace original IP/port within the contact header of REGISTER requests.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>				Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
	Option	Description										
	<i>disable</i>	Disable status.										
<i>enable</i>	Enable status.											
register-rate	REGISTER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
register-rate-track	Track the packet protocol field.	option	-	none								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
rfc2543-branch	Enable/disable support via branch compliant with RFC 2543.	option	-	disable
	Option Description			
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
rtp	Enable/disable create pinholes for RTP traffic to traverse firewall.	option	-	enable
	Option Description			
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	Option Description			
	<i>high</i>	High encryption. Allow only AES and ChaCha.		
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
ssl-auth-client	Require a client certificate and authenticate it with the peer/peergrp.	string	Maximum length: 35	
ssl-auth-server	Authenticate the server's certificate with the peer/peergrp.	string	Maximum length: 35	
ssl-client-certificate	Name of Certificate to offer to server if requested.	string	Maximum length: 35	
ssl-client-renegotiation	Allow/block client renegotiation by server.	option	-	allow
	Option Description			
	<i>allow</i>	Allow a SSL client to renegotiate.		
	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>secure</i></td><td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td></tr></table>	Option	Description	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.											
	Option	Description														
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.															
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-	tls-1.3												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description														
	<i>ssl-3.0</i>	SSL 3.0.														
	<i>tls-1.0</i>	TLS 1.0.														
	<i>tls-1.1</i>	TLS 1.1.														
	<i>tls-1.2</i>	TLS 1.2.														
<i>tls-1.3</i>	TLS 1.3.															
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description														
	<i>ssl-3.0</i>	SSL 3.0.														
	<i>tls-1.0</i>	TLS 1.0.														
	<i>tls-1.1</i>	TLS 1.1.														
	<i>tls-1.2</i>	TLS 1.2.														
<i>tls-1.3</i>	TLS 1.3.															
ssl-mode	SSL/TLS mode for encryption & decryption of traffic.	option	-	off												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>off</i></td><td>No SSL.</td></tr><tr><td><i>full</i></td><td>Client to FortiGate and FortiGate to Server SSL.</td></tr></table>	Option	Description	<i>off</i>	No SSL.	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.									
	Option	Description														
	<i>off</i>	No SSL.														
<i>full</i>	Client to FortiGate and FortiGate to Server SSL.															
ssl-pfs	SSL Perfect Forward Secrecy.	option	-	allow												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>require</i></td><td>PFS mandatory.</td></tr><tr><td><i>deny</i></td><td>PFS rejected.</td></tr><tr><td><i>allow</i></td><td>PFS allowed.</td></tr></table>	Option	Description	<i>require</i>	PFS mandatory.	<i>deny</i>	PFS rejected.	<i>allow</i>	PFS allowed.							
	Option	Description														
	<i>require</i>	PFS mandatory.														
	<i>deny</i>	PFS rejected.														
<i>allow</i>	PFS allowed.															

Parameter	Description	Type	Size	Default								
ssl-send-empty-frags	Send empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send empty fragments.</td></tr><tr><td><i>disable</i></td><td>Do not send empty fragments.</td></tr></table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.					
Option	Description											
<i>enable</i>	Send empty fragments.											
<i>disable</i>	Do not send empty fragments.											
ssl-server-certificate	Name of Certificate return to the client in every SSL connection.	string	Maximum length: 35									
status	Enable/disable SIP.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.					
Option	Description											
<i>disable</i>	Disable status.											
<i>enable</i>	Enable status.											
strict-register	Enable/disable only allow the registrar to connect.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.					
Option	Description											
<i>disable</i>	Disable status.											
<i>enable</i>	Enable status.											
subscribe-rate	SUBSCRIBE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
subscribe-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
unknown-header	Action for unknown SIP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.							
Option	Description											
<i>discard</i>	Discard malformed messages.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
update-rate	UPDATE request rate limit (per second, per policy).	integer	Minimum value: 0 0 Maximum value: 4294967295	0
update-rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		

vpn

This section includes syntax for the following commands:

- [config vpn certificate ca on page 2121](#)
- [config vpn certificate crl on page 2123](#)
- [config vpn certificate hsm-local on page 2125](#)
- [config vpn certificate local on page 2129](#)
- [config vpn certificate ocsf-server on page 2134](#)
- [config vpn certificate remote on page 2135](#)
- [config vpn certificate setting on page 2136](#)
- [config vpn ipsec concentrator on page 2142](#)
- [config vpn ipsec fec on page 2142](#)
- [config vpn ipsec manualkey-interface on page 2146](#)
- [config vpn ipsec manualkey on page 2144](#)
- [config vpn ipsec phase1-interface on page 2179](#)
- [config vpn ipsec phase1 on page 2148](#)
- [config vpn ipsec phase2-interface on page 2230](#)
- [config vpn ipsec phase2 on page 2216](#)
- [config vpn kmip-server on page 2244](#)
- [config vpn l2tp on page 2246](#)
- [config vpn pptp on page 2248](#)
- [config vpn qkd on page 2248](#)
- [config vpn ssl settings on page 2250](#)
- [config vpn ssl web portal on page 2262](#)
- [config vpn ssl web realm on page 2278](#)
- [config vpn ssl web user-bookmark on page 2280](#)
- [config vpn ssl web user-group-bookmark on page 2288](#)

config vpn certificate ca

CA certificate.

```
config vpn certificate ca
  Description: CA certificate.
  edit <name>
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set ca {user}
    set ca-identifier {string}
```

```

set est-url {string}
set fabric-ca [disable|enable]
set obsolete [disable|enable]
set range [global|vdom]
set scep-url {string}
set source [factory|user|...]
set source-ip {ipv4-address}
set ssl-inspection-trusted [enable|disable]
next
end

```

config vpn certificate ca

Parameter	Description	Type	Size	Default
auto-update-days	Number of days to wait before requesting an updated CA certificate (0 - 4294967295, 0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated (0 - 4294967295, 0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
ca	CA certificate as a PEM file.	user	Not Specified	
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255	
est-url	URL of the EST server.	string	Maximum length: 255	
fabric-ca	Enable/disable synchronization of CA across Security Fabric.	option	-	disable
	Option		Description	
	<i>disable</i>		Disable synchronization of CA across Security Fabric.	
	<i>enable</i>		Enable synchronization of CA across Security Fabric.	
name	Name.	string	Maximum length: 79	
obsolete	Enable/disable this CA as obsoleted.	option	-	disable
	Option		Description	
	<i>disable</i>		Alive.	
	<i>enable</i>		Obsolete.	

Parameter	Description	Type	Size	Default
range	Either global or VDOM IP address range for the CA certificate.	option	-	vdom
	Option	Description		
	<i>global</i>	Global range.		
	<i>vdom</i>	VDOM IP address range.		
scep-url	URL of the SCEP server.	string	Maximum length: 255	
source	CA certificate source type.	option	-	user
	Option	Description		
	<i>factory</i>	Factory installed certificate.		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable
	Option	Description		
	<i>enable</i>	Trusted CA for SSL inspection.		
	<i>disable</i>	Untrusted CA for SSL inspection.		

config vpn certificate crl

Certificate Revocation List as a PEM file.

```

config vpn certificate crl
  Description: Certificate Revocation List as a PEM file.
  edit <name>
    set crl {user}
    set http-url {string}
    set ldap-password {password}
    set ldap-server {string}
    set ldap-username {string}
    set range [global|vdom]
    set scep-cert {string}
    set scep-url {string}
    set source [factory|user|...]

```

```

    set source-ip {ipv4-address}
    set update-interval {integer}
    set update-vdom {string}
next
end

```

config vpn certificate crl

Parameter	Description	Type	Size	Default								
crl	Certificate Revocation List as a PEM file.	user	Not Specified									
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255									
ldap-password	LDAP server user password.	password	Not Specified									
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35									
ldap-username	LDAP server user name.	string	Maximum length: 63									
name	Name.	string	Maximum length: 35									
range	Either global or VDOM IP address range for the certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>				Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.		
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL								
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255									
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>				Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0								

Parameter	Description	Type	Size	Default
update-interval	Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root

config vpn certificate hsm-local

Local certificates whose keys are stored on HSM.

```

config vpn certificate hsm-local
    Description: Local certificates whose keys are stored on HSM.
    edit <name>
        set api-version [unknown|gch-default]
        set certificate {user}
        set comments {string}
        set gch-cloud-service-name {string}
        set gch-cryptokey {string}
        set gch-cryptokey-algorithm [rsa-sign-pkcs1-2048-sha256|rsa-sign-pkcs1-3072-sha256|...]
        set gch-cryptokey-version {string}
        set gch-keyring {string}
        set gch-location {string}
        set gch-project {string}
        set gch-url {string}
        set range [global|vdom]
        set source [factory|user|...]
        set vendor [unknown|gch]
    next
end

```

config vpn certificate hsm-local

Parameter	Description	Type	Size	Default						
api-version	API version for communicating with HSM.	option	-	unknown						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>unknown</td><td>Unknown API version.</td></tr><tr><td>gch-default</td><td>Google Cloud HSM default API.</td></tr></table>				Option	Description	unknown	Unknown API version.	gch-default	Google Cloud HSM default API.
Option	Description									
unknown	Unknown API version.									
gch-default	Google Cloud HSM default API.									

Parameter	Description	Type	Size	Default
certificate	PEM format certificate.	user	Not Specified	
comments	Comment.	string	Maximum length: 511	
gcloud-service-name	Cloud service config name to generate access token.	string	Maximum length: 35	
gch-cryptokey	Google Cloud HSM cryptokey.	string	Maximum length: 63	
gch-cryptokey-algorithm	Google Cloud HSM cryptokey algorithm.	option	-	rsa-sign-pkcs1-2048-sha256

Option	Description
<i>rsa-sign-pkcs1-2048-sha256</i>	2048 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.
<i>rsa-sign-pkcs1-3072-sha256</i>	3072 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.
<i>rsa-sign-pkcs1-4096-sha256</i>	4096 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>rsa-sign-pkcs1-4096-sha512</td><td>4096 bit RSA - PKCS#1 v1.5 padding - SHA512 Digest.</td></tr><tr><td>rsa-sign-pss-2048-sha256</td><td>2048 bit RSA - PSS padding - SHA256 Digest.</td></tr><tr><td>rsa-sign-pss-3072-sha256</td><td>3072 bit RSA - PSS padding - SHA256 Digest.</td></tr><tr><td>rsa-sign-pss-4096-sha256</td><td>4096 bit RSA - PSS padding - SHA256 Digest.</td></tr><tr><td>rsa-sign-pss-4096-sha512</td><td>4096 bit RSA - PSS padding - SHA256 Digest.</td></tr><tr><td>ec-sign-p256-sha256</td><td>Elliptic Curve P-256 - SHA256 Digest.</td></tr><tr><td>ec-sign-p384-sha384</td><td>Elliptic Curve P-384 - SHA384 Digest.</td></tr><tr><td>ec-sign-secp256k1-sha256</td><td>Elliptic Curvesecp256k1 - SHA256 Digest.</td></tr></table>	Option	Description	rsa-sign-pkcs1-4096-sha512	4096 bit RSA - PKCS#1 v1.5 padding - SHA512 Digest.	rsa-sign-pss-2048-sha256	2048 bit RSA - PSS padding - SHA256 Digest.	rsa-sign-pss-3072-sha256	3072 bit RSA - PSS padding - SHA256 Digest.	rsa-sign-pss-4096-sha256	4096 bit RSA - PSS padding - SHA256 Digest.	rsa-sign-pss-4096-sha512	4096 bit RSA - PSS padding - SHA256 Digest.	ec-sign-p256-sha256	Elliptic Curve P-256 - SHA256 Digest.	ec-sign-p384-sha384	Elliptic Curve P-384 - SHA384 Digest.	ec-sign-secp256k1-sha256	Elliptic Curvesecp256k1 - SHA256 Digest.			
	Option	Description																				
	rsa-sign-pkcs1-4096-sha512	4096 bit RSA - PKCS#1 v1.5 padding - SHA512 Digest.																				
	rsa-sign-pss-2048-sha256	2048 bit RSA - PSS padding - SHA256 Digest.																				
	rsa-sign-pss-3072-sha256	3072 bit RSA - PSS padding - SHA256 Digest.																				
	rsa-sign-pss-4096-sha256	4096 bit RSA - PSS padding - SHA256 Digest.																				
	rsa-sign-pss-4096-sha512	4096 bit RSA - PSS padding - SHA256 Digest.																				
	ec-sign-p256-sha256	Elliptic Curve P-256 - SHA256 Digest.																				
ec-sign-p384-sha384	Elliptic Curve P-384 - SHA384 Digest.																					
ec-sign-secp256k1-sha256	Elliptic Curvesecp256k1 - SHA256 Digest.																					
gch-cryptokey-version	Google Cloud HSM cryptokey version.	string	Maximum length: 31																			
gch-keyring	Google Cloud HSM keyring.	string	Maximum length: 63																			
gch-location	Google Cloud HSM location.	string	Maximum length: 63																			

Parameter	Description	Type	Size	Default								
gch-project	Google Cloud HSM project ID.	string	Maximum length: 31									
gch-url	Google Cloud HSM key URL (e.g. "https://cloudkms.googleapis.com/v1/projects/sampleproject/locations/samplelocation/keyRings/samplekeyring/cryptoKeys/sampleKeyName/cryptoKeyVersions/1"). Read-only.	string	Maximum length: 1024									
name	Name.	string	Maximum length: 35									
range	Either a global or VDOM IP address range for the certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>global</td><td>Global range.</td></tr><tr><td>vdom</td><td>VDOM IP address range.</td></tr></table>				Option	Description	global	Global range.	vdom	VDOM IP address range.		
Option	Description											
global	Global range.											
vdom	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>factory</td><td>Factory installed certificate.</td></tr><tr><td>user</td><td>User generated certificate.</td></tr><tr><td>bundle</td><td>Bundle file certificate.</td></tr></table>				Option	Description	factory	Factory installed certificate.	user	User generated certificate.	bundle	Bundle file certificate.
Option	Description											
factory	Factory installed certificate.											
user	User generated certificate.											
bundle	Bundle file certificate.											
vendor	HSM vendor.	option	-	unknown								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unknown</i></td><td>Unknown type of HSM.</td></tr><tr><td><i>gch</i></td><td>Google Cloud HSM.</td></tr></table>	Option	Description	<i>unknown</i>	Unknown type of HSM.	<i>gch</i>	Google Cloud HSM.			
Option	Description									
<i>unknown</i>	Unknown type of HSM.									
<i>gch</i>	Google Cloud HSM.									

config vpn certificate local

Local keys and certificates.

```

config vpn certificate local
    Description: Local keys and certificates.
    edit <name>
        set acme-ca-url {string}
        set acme-domain {string}
        set acme-eab-key-hmac {password}
        set acme-eab-key-id {var-string}
        set acme-email {string}
        set acme-renew-window {integer}
        set acme-rsa-key-size {integer}
        set auto-regenerate-days {integer}
        set auto-regenerate-days-warning {integer}
        set ca-identifier {string}
        set certificate {user}
        set cmp-path {string}
        set cmp-regeneration-method [keyupdate|renewal]
        set cmp-server {string}
        set cmp-server-cert {string}
        set comments {string}
        set csr {user}
        set enroll-protocol [none|scep|...]
        set est-ca-id {string}
        set est-client-cert {string}
        set est-http-password {password}
        set est-http-username {string}
        set est-regeneration-method [create-new-key|use-existing-key]
        set est-server {string}
        set est-server-cert {string}
        set est-srp-password {password}
        set est-srp-username {string}
        set ike-localid {string}
        set ike-localid-type [asn1dn|fqdn]
        set name-encoding [printable|utf8]
        set password {password}
        set private-key {user}
        set private-key-retain [enable|disable]

```

```

    set range [global|vdom]
    set scep-password {password}
    set scep-url {string}
    set source [factory|user|...]
    set source-ip {ipv4-address}
    set state {user}
next
end

```

config vpn certificate local

Parameter	Description	Type	Size	Default
acme-ca-url	The URL for the ACME CA server (Let's Encrypt is the default provider).	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory
acme-domain	A valid domain that resolves to this FortiGate unit.	string	Maximum length: 255	
acme-eab-key-hmac	External Account Binding HMAC Key (URL-encoded base64).	password	Not Specified	
acme-eab-key-id	External Account Binding Key ID (optional setting).	var-string	Maximum length: 255	
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255	
acme-renew-window	Beginning of the renewal window (in days before certificate expiration, 30 by default).	integer	Minimum value: 1 Maximum value: 100	30
acme-rsa-key-size	Length of the RSA private key of the generated cert (Minimum 2048 bits).	integer	Minimum value: 2048 Maximum value: 4096	2048
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default												
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0												
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255													
certificate	PEM format certificate.	user	Not Specified													
cmp-path	Path location inside CMP server.	string	Maximum length: 255													
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>keyupate</td><td>Key Update.</td></tr><tr><td>renewal</td><td>Renewal.</td></tr></table>				Option	Description	keyupate	Key Update.	renewal	Renewal.						
Option	Description															
keyupate	Key Update.															
renewal	Renewal.															
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63													
cmp-server-cert	CMP server certificate.	string	Maximum length: 79													
comments	Comment.	string	Maximum length: 511													
csr	Certificate Signing Request.	user	Not Specified													
enroll-protocol	Certificate enrollment protocol.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>None (default).</td></tr><tr><td>scep</td><td>Simple Certificate Enrollment Protocol.</td></tr><tr><td>cmpv2</td><td>Certificate Management Protocol Version 2.</td></tr><tr><td>acme2</td><td>Automated Certificate Management Environment Version 2.</td></tr><tr><td>est</td><td>Enrollment over Secure Transport.</td></tr></table>				Option	Description	none	None (default).	scep	Simple Certificate Enrollment Protocol.	cmpv2	Certificate Management Protocol Version 2.	acme2	Automated Certificate Management Environment Version 2.	est	Enrollment over Secure Transport.
Option	Description															
none	None (default).															
scep	Simple Certificate Enrollment Protocol.															
cmpv2	Certificate Management Protocol Version 2.															
acme2	Automated Certificate Management Environment Version 2.															
est	Enrollment over Secure Transport.															
est-ca-id	CA identifier of the CA server for signing via EST.	string	Maximum length: 255													

Parameter	Description	Type	Size	Default						
est-client-cert	Certificate used to authenticate this FortiGate to EST server.	string	Maximum length: 79							
est-http-password	HTTP Authentication password for signing via EST.	password	Not Specified							
est-http-username	HTTP Authentication username for signing via EST.	string	Maximum length: 63							
est-regeneration-method	EST behavioral options during re-enrollment.	option	-	create-new-key						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>create-new-key</td><td>Create new private key during re-enrollment.</td></tr><tr><td>use-existing-key</td><td>Reuse existing private key during re-enrollment.</td></tr></table>				Option	Description	create-new-key	Create new private key during re-enrollment.	use-existing-key	Reuse existing private key during re-enrollment.
Option	Description									
create-new-key	Create new private key during re-enrollment.									
use-existing-key	Reuse existing private key during re-enrollment.									
est-server	Address and port for EST server (e.g. https://example.com:1234).	string	Maximum length: 255							
est-server-cert	EST server's certificate must be verifiable by this certificate to be authenticated.	string	Maximum length: 79							
est-srp-password	EST SRP authentication password.	password	Not Specified							
est-srp-username	EST SRP authentication username.	string	Maximum length: 63							
ike-localid	Local ID the FortiGate uses for authentication as a VPN client.	string	Maximum length: 63							
ike-localid-type	IKE local ID type.	option	-	asn1dn						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>asn1dn</td><td>ASN.1 distinguished name.</td></tr><tr><td>fqdn</td><td>Fully qualified domain name.</td></tr></table>				Option	Description	asn1dn	ASN.1 distinguished name.	fqdn	Fully qualified domain name.
Option	Description									
asn1dn	ASN.1 distinguished name.									
fqdn	Fully qualified domain name.									

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
name-encoding	Name encoding method for auto-regeneration.	option	-	printable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>printable</i></td><td>Printable encoding (default).</td></tr><tr><td><i>utf8</i></td><td>UTF-8 encoding.</td></tr></table>	Option	Description	<i>printable</i>	Printable encoding (default).	<i>utf8</i>	UTF-8 encoding.					
Option	Description											
<i>printable</i>	Printable encoding (default).											
<i>utf8</i>	UTF-8 encoding.											
password	Password as a PEM file.	password	Not Specified									
private-key	PEM format key encrypted with a password.	user	Not Specified									
private-key-retain	Enable/disable retention of private key during SCEP renewal (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the existing private key during SCEP renewal.</td></tr><tr><td><i>disable</i></td><td>Generate a new private key during SCEP renewal.</td></tr></table>	Option	Description	<i>enable</i>	Keep the existing private key during SCEP renewal.	<i>disable</i>	Generate a new private key during SCEP renewal.					
Option	Description											
<i>enable</i>	Keep the existing private key during SCEP renewal.											
<i>disable</i>	Generate a new private key during SCEP renewal.											
range	Either a global or VDOM IP address range for the certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified									
scep-url	SCEP server URL.	string	Maximum length: 255									
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											

Parameter	Description	Type	Size	Default
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
state	Certificate Signing Request State. Read-only.	user	Not Specified	

config vpn certificate ocsf-server

OCSP server configuration.

```

config vpn certificate ocsf-server
  Description: OCSP server configuration.
  edit <name>
    set cert {string}
    set secondary-cert {string}
    set secondary-url {string}
    set source-ip {string}
    set unavail-action [revoke|ignore]
    set url {string}
  next
end

```

config vpn certificate ocsf-server

Parameter	Description	Type	Size	Default
cert	OCSP server certificate.	string	Maximum length: 127	
name	OCSP server entry name.	string	Maximum length: 35	
secondary-cert	Secondary OCSP server certificate.	string	Maximum length: 127	
secondary-url	Secondary OCSP server URL.	string	Maximum length: 127	
source-ip	Source IP address for dynamic AIA and OCSP queries.	string	Maximum length: 63	
unavail-action	Action when server is unavailable (revoke the certificate or ignore the result of the check).	option	-	revoke

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>revoke</i>	Revoke certificate if server is unavailable.		
	<i>ignore</i>	Ignore OCSP check if server is unavailable.		
url	OCSP server URL.	string	Maximum length: 127	

config vpn certificate remote

Remote certificate as a PEM file.

```
config vpn certificate remote
  Description: Remote certificate as a PEM file.
  edit <name>
    set range [global|vdom]
    set remote {user}
    set source [factory|user|...]
  next
end
```

config vpn certificate remote

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
range	Either the global or VDOM IP address range for the remote certificate.	option	-	vdom
	Option	Description		
	<i>global</i>	Global range.		
	<i>vdom</i>	VDOM IP address range.		
remote	Remote certificate.	user	Not Specified	
source	Remote certificate source type.	option	-	user
	Option	Description		
	<i>factory</i>	Factory installed certificate.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		

config vpn certificate setting

VPN certificate setting.

```

config vpn certificate setting
    Description: VPN certificate setting.
    set cert-expire-warning {integer}
    set certname-dsa1024 {string}
    set certname-dsa2048 {string}
    set certname-ecdsa256 {string}
    set certname-ecdsa384 {string}
    set certname-ecdsa521 {string}
    set certname-ed25519 {string}
    set certname-ed448 {string}
    set certname-rsa1024 {string}
    set certname-rsa2048 {string}
    set certname-rsa4096 {string}
    set check-ca-cert [enable|disable]
    set check-ca-chain [enable|disable]
    set cmp-key-usage-checking [enable|disable]
    set cmp-save-extra-certs [enable|disable]
    set cn-allow-multi [disable|enable]
    set cn-match [substring|value]
    config crl-verification
        Description: CRL verification options.
        set chain-crl-absence [ignore|revoke]
        set expiry [ignore|revoke]
        set leaf-crl-absence [ignore|revoke]
    end
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set oasp-default-server {string}
    set oasp-option [certificate|server]
    set oasp-status [enable|mandatory|...]
    set proxy {string}
    set proxy-password {password}
    set proxy-port {integer}
    set proxy-username {string}
    set source-ip {string}
    set ssl-min-protocol-version [default|SSLv3|...]
    set strict-oasp-check [enable|disable]
    set subject-match [substring|value]

```



```

set subject-set [subset|superset]
set vrf-select {integer}
end

```

config vpn certificate setting

Parameter	Description	Type	Size	Default
cert-expire-warning	Number of days before a certificate expires to send a warning. Set to 0 to disable sending of the warning (0 - 100, default = 14).	integer	Minimum value: 0 Maximum value: 100	14
certname-dsa1024	1024 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA1024
certname-dsa2048	2048 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA2048
certname-ecdsa256	256 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA256
certname-ecdsa384	384 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA384
certname-ecdsa521	521 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA521
certname-ed25519	253 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED25519
certname-ed448	456 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED448
certname-rsa1024	1024 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA1024
certname-rsa2048	2048 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA2048
certname-rsa4096	4096 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA4096

Parameter	Description	Type	Size	Default						
check-ca-cert	Enable/disable verification of the user certificate and pass authentication if any CA in the chain is trusted (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of the user certificate.</td></tr><tr><td><i>disable</i></td><td>Disable verification of the user certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable verification of the user certificate.	<i>disable</i>	Disable verification of the user certificate.			
Option	Description									
<i>enable</i>	Enable verification of the user certificate.									
<i>disable</i>	Disable verification of the user certificate.									
check-ca-chain	Enable/disable verification of the entire certificate chain and pass authentication only if the chain is complete and all of the CAs in the chain are trusted (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of the entire certificate chain.</td></tr><tr><td><i>disable</i></td><td>Disable verification of the entire certificate chain.</td></tr></table>	Option	Description	<i>enable</i>	Enable verification of the entire certificate chain.	<i>disable</i>	Disable verification of the entire certificate chain.			
Option	Description									
<i>enable</i>	Enable verification of the entire certificate chain.									
<i>disable</i>	Disable verification of the entire certificate chain.									
cmp-key-usage-checking	Enable/disable server certificate key usage checking in CMP mode (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server certificate key usage checking in CMP mode.</td></tr><tr><td><i>disable</i></td><td>Disable server certificate key usage checking in CMP mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable server certificate key usage checking in CMP mode.	<i>disable</i>	Disable server certificate key usage checking in CMP mode.			
Option	Description									
<i>enable</i>	Enable server certificate key usage checking in CMP mode.									
<i>disable</i>	Disable server certificate key usage checking in CMP mode.									
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable saving extra certificates in CMP mode.</td></tr><tr><td><i>disable</i></td><td>Disable saving extra certificates in CMP mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable saving extra certificates in CMP mode.	<i>disable</i>	Disable saving extra certificates in CMP mode.			
Option	Description									
<i>enable</i>	Enable saving extra certificates in CMP mode.									
<i>disable</i>	Disable saving extra certificates in CMP mode.									
cn-allow-multi	When searching for a matching certificate, allow multiple CN fields in certificate subject name (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Does not allow multiple CN entries in certificate matching.</td></tr><tr><td><i>enable</i></td><td>Allow multiple CN entries in certificate matching.</td></tr></table>	Option	Description	<i>disable</i>	Does not allow multiple CN entries in certificate matching.	<i>enable</i>	Allow multiple CN entries in certificate matching.			
Option	Description									
<i>disable</i>	Does not allow multiple CN entries in certificate matching.									
<i>enable</i>	Allow multiple CN entries in certificate matching.									

Parameter	Description	Type	Size	Default								
cn-match	When searching for a matching certificate, control how to do CN value matching with certificate subject name (default = substring).	option	-	substring								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>substring</td><td>Find a match if the name being searched for is a part or the same as a certificate CN.</td></tr><tr><td>value</td><td>Find a match if the name being searched for is same as a certificate CN.</td></tr></table>	Option	Description	substring	Find a match if the name being searched for is a part or the same as a certificate CN.	value	Find a match if the name being searched for is same as a certificate CN.					
Option	Description											
substring	Find a match if the name being searched for is a part or the same as a certificate CN.											
value	Find a match if the name being searched for is same as a certificate CN.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
ocsp-default-server	Default OCSP server.	string	Maximum length: 35									
ocsp-option	Specify whether the OCSP URL is from certificate or configured OCSP server.	option	-	server								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>certificate</td><td>Use URL from certificate.</td></tr><tr><td>server</td><td>Use URL from configured OCSP server.</td></tr></table>	Option	Description	certificate	Use URL from certificate.	server	Use URL from configured OCSP server.					
Option	Description											
certificate	Use URL from certificate.											
server	Use URL from configured OCSP server.											
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>OCSP is performed if CRL is not checked.</td></tr><tr><td>mandatory</td><td>If cert is not revoked by CRL, OCSP is performed.</td></tr><tr><td>disable</td><td>OCSP is not performed.</td></tr></table>	Option	Description	enable	OCSP is performed if CRL is not checked.	mandatory	If cert is not revoked by CRL, OCSP is performed.	disable	OCSP is not performed.			
Option	Description											
enable	OCSP is performed if CRL is not checked.											
mandatory	If cert is not revoked by CRL, OCSP is performed.											
disable	OCSP is not performed.											
proxy	Proxy server FQDN or IP for OCSP/CA queries during certificate verification.	string	Maximum length: 127									

Parameter	Description	Type	Size	Default														
proxy-password	Proxy server password.	password	Not Specified															
proxy-port	Proxy server port (1 - 65535, default = 8080).	integer	Minimum value: 1 Maximum value: 65535	8080														
proxy-username	Proxy server user name.	string	Maximum length: 63															
source-ip	Source IP address for dynamic AIA and OCSP queries.	string	Maximum length: 63															
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>				Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.
Option	Description																	
default	Follow system global setting.																	
SSLv3	SSLv3.																	
TLSv1	TLSv1.																	
TLSv1-1	TLSv1.1.																	
TLSv1-2	TLSv1.2.																	
TLSv1-3	TLSv1.3.																	
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable strict mode OCSP checking.</td></tr><tr><td>disable</td><td>Disable strict mode OCSP checking.</td></tr></table>				Option	Description	enable	Enable strict mode OCSP checking.	disable	Disable strict mode OCSP checking.								
Option	Description																	
enable	Enable strict mode OCSP checking.																	
disable	Disable strict mode OCSP checking.																	
subject-match	When searching for a matching certificate, control how to do RDN value matching with certificate subject name (default = substring).	option	-	substring														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>substring</td><td>Find a match if the name being searched for is a part or the same as a certificate subject RDN.</td></tr><tr><td>value</td><td>Find a match if the name being searched for is same as a certificate subject RDN.</td></tr></table>				Option	Description	substring	Find a match if the name being searched for is a part or the same as a certificate subject RDN.	value	Find a match if the name being searched for is same as a certificate subject RDN.								
Option	Description																	
substring	Find a match if the name being searched for is a part or the same as a certificate subject RDN.																	
value	Find a match if the name being searched for is same as a certificate subject RDN.																	

Parameter	Description	Type	Size	Default						
subject-set	When searching for a matching certificate, control how to do RDN set matching with certificate subject name (default = subset).	option	-	subset						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subset</i></td><td>Find a match if the name being searched for is a subset of a certificate subject.</td></tr><tr><td><i>superset</i></td><td>Find a match if the name being searched for is a superset of a certificate subject.</td></tr></table>				Option	Description	<i>subset</i>	Find a match if the name being searched for is a subset of a certificate subject.	<i>superset</i>	Find a match if the name being searched for is a superset of a certificate subject.
Option	Description									
<i>subset</i>	Find a match if the name being searched for is a subset of a certificate subject.									
<i>superset</i>	Find a match if the name being searched for is a superset of a certificate subject.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0						

config crt-verification

Parameter	Description	Type	Size	Default						
chain-crl-absence	CRL verification option when CRL of any certificate in chain is absent (default = ignore).	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>CRL verification is ignored if CRL of any certificate in chain is absent.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL of any certificate in chain is absent.</td></tr></table>	Option	Description	ignore	CRL verification is ignored if CRL of any certificate in chain is absent.	revoke	Certificate will be revoked if CRL of any certificate in chain is absent.			
Option	Description									
ignore	CRL verification is ignored if CRL of any certificate in chain is absent.									
revoke	Certificate will be revoked if CRL of any certificate in chain is absent.									
expiry	CRL verification option when CRL is expired (default = ignore).	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>Certificate status will be verified even if CRL is expired.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL is expired.</td></tr></table>	Option	Description	ignore	Certificate status will be verified even if CRL is expired.	revoke	Certificate will be revoked if CRL is expired.			
Option	Description									
ignore	Certificate status will be verified even if CRL is expired.									
revoke	Certificate will be revoked if CRL is expired.									
leaf-crl-absence	CRL verification option when leaf CRL is absent (default = ignore).	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>CRL verification against leaf certificate is ignored if CRL is absent.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL of leaf certificate is absent.</td></tr></table>	Option	Description	ignore	CRL verification against leaf certificate is ignored if CRL is absent.	revoke	Certificate will be revoked if CRL of leaf certificate is absent.			
Option	Description									
ignore	CRL verification against leaf certificate is ignored if CRL is absent.									
revoke	Certificate will be revoked if CRL of leaf certificate is absent.									

config vpn ipsec concentrator

Concentrator configuration.

```
config vpn ipsec concentrator
  Description: Concentrator configuration.
  edit <id>
    set member <name1>, <name2>, ...
    set name {string}
    set src-check [disable|enable]
  next
end
```

config vpn ipsec concentrator

Parameter	Description	Type	Size	Default
id	Concentrator ID (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	0
member <name>	Names of up to 3 VPN tunnels to add to the concentrator. Member name.	string	Maximum length: 79	
name	Concentrator name.	string	Maximum length: 35	
src-check	Enable to check source address of phase 2 selector. Disable to check only the destination selector.	option	-	disable
		Option	Description	
		<i>disable</i>	Ignore source selector when choosing tunnel.	
		<i>enable</i>	Use source selector to choose tunnel.	

config vpn ipsec fec

Configure Forward Error Correction (FEC) mapping profiles.

```
config vpn ipsec fec
  Description: Configure Forward Error Correction (FEC) mapping profiles.
  edit <name>
    config mappings
```

```

Description: FEC redundancy mapping table.
edit <seqno>
    set bandwidth-bi-threshold {integer}
    set bandwidth-down-threshold {integer}
    set bandwidth-up-threshold {integer}
    set base {integer}
    set latency-threshold {integer}
    set packet-loss-threshold {integer}
    set redundant {integer}
next
end
next
end

```

config vpn ipsec fec

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	

config mappings

Parameter	Description	Type	Size	Default
bandwidth-bi-threshold	Apply FEC parameters when available bi-bandwidth is $\geq$ threshold (kbps, 0 means no threshold).	integer	Minimum value: 0 Maximum value: 4294967295	0
bandwidth-down-threshold	Apply FEC parameters when available down bandwidth is $\geq$ threshold (kbps, 0 means no threshold).	integer	Minimum value: 0 Maximum value: 4294967295	0
bandwidth-up-threshold	Apply FEC parameters when available up bandwidth is $\geq$ threshold (kbps, 0 means no threshold).	integer	Minimum value: 0 Maximum value: 4294967295	0
base	Number of base FEC packets (1 - 20).	integer	Minimum value: 1 Maximum value: 20	0
latency-threshold	Apply FEC parameters when latency is $\leq$ threshold (0 means no threshold).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
packet-loss-threshold	Apply FEC parameters when packet loss is >= threshold (0 - 100, 0 means no threshold).	integer	Minimum value: 0 Maximum value: 100	0
redundant	Number of redundant FEC packets (1 - 5).	integer	Minimum value: 1 Maximum value: 5	0
seqno	Sequence number (1 - 64).	integer	Minimum value: 0 Maximum value: 64	0

config vpn ipsec manualkey

Configure IPsec manual keys.

```

config vpn ipsec manualkey
  Description: Configure IPsec manual keys.
  edit <name>
    set authentication [null|md5|...]
    set authkey {user}
    set enckey {user}
    set encryption [null|des|...]
    set interface {string}
    set local-gw {ipv4-address-any}
    set localspi {user}
    set npu-offload [enable|disable]
    set remote-gw {ipv4-address}
    set remotespi {user}
  next
end

```

config vpn ipsec manualkey

Parameter	Description	Type	Size	Default								
authentication	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-	null								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null</i></td><td>Null.</td></tr><tr><td><i>md5</i></td><td>MD5.</td></tr><tr><td><i>sha1</i></td><td>SHA1.</td></tr></table>				Option	Description	<i>null</i>	Null.	<i>md5</i>	MD5.	<i>sha1</i>	SHA1.
	Option	Description										
	<i>null</i>	Null.										
	<i>md5</i>	MD5.										
<i>sha1</i>	SHA1.											

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha256</td><td>SHA256.</td></tr><tr><td>sha384</td><td>SHA384.</td></tr><tr><td>sha512</td><td>SHA512.</td></tr></table>	Option	Description	sha256	SHA256.	sha384	SHA384.	sha512	SHA512.																	
	Option	Description																								
	sha256	SHA256.																								
	sha384	SHA384.																								
sha512	SHA512.																									
authkey	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																							
enckey	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																							
encryption	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-	null																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>null</td><td>Null.</td></tr><tr><td>des</td><td>DES.</td></tr><tr><td>3des</td><td>3DES.</td></tr><tr><td>aes128</td><td>AES128.</td></tr><tr><td>aes192</td><td>AES192.</td></tr><tr><td>aes256</td><td>AES256.</td></tr><tr><td>aria128</td><td>ARIA128.</td></tr><tr><td>aria192</td><td>ARIA192.</td></tr><tr><td>aria256</td><td>ARIA256.</td></tr><tr><td>seed</td><td>Seed.</td></tr></table>	Option	Description	null	Null.	des	DES.	3des	3DES.	aes128	AES128.	aes192	AES192.	aes256	AES256.	aria128	ARIA128.	aria192	ARIA192.	aria256	ARIA256.	seed	Seed.			
	Option	Description																								
	null	Null.																								
	des	DES.																								
	3des	3DES.																								
	aes128	AES128.																								
	aes192	AES192.																								
	aes256	AES256.																								
	aria128	ARIA128.																								
	aria192	ARIA192.																								
	aria256	ARIA256.																								
seed	Seed.																									
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15																							
local-gw	Local gateway.	ipv4-address-any	Not Specified	0.0.0.0																						
localspi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified																							
name	IPsec tunnel name.	string	Maximum length: 35																							
npu-offload *	Enable/disable NPU offloading.	option	-	enable																						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable NPU offloading.		
	<i>disable</i>	Disable NPU offloading.		
remote-gw	Peer gateway.	ipv4-address	Not Specified	0.0.0.0
remotespi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified	

* This parameter may not exist in some models.

config vpn ipsec manualkey-interface

Configure IPsec manual keys.

```

config vpn ipsec manualkey-interface
  Description: Configure IPsec manual keys.
  edit <name>
    set addr-type [4|6]
    set auth-alg [null|md5|...]
    set auth-key {user}
    set enc-alg [null|des|...]
    set enc-key {user}
    set interface {string}
    set ip-version [4|6]
    set local-gw {ipv4-address-any}
    set local-gw6 {ipv6-address}
    set local-spi {user}
    set npu-offload [enable|disable]
    set remote-gw {ipv4-address}
    set remote-gw6 {ipv6-address}
    set remote-spi {user}
  next
end

```

config vpn ipsec manualkey-interface

Parameter	Description	Type	Size	Default
addr-type	IP version to use for IP packets.	option	-	4

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for IP packets.</td></tr><tr><td>6</td><td>Use IPv6 addressing for IP packets.</td></tr></table>	Option	Description	4	Use IPv4 addressing for IP packets.	6	Use IPv6 addressing for IP packets.																			
	Option	Description																								
	4	Use IPv4 addressing for IP packets.																								
6	Use IPv6 addressing for IP packets.																									
auth-alg	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-	null																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>null</td><td>null</td></tr><tr><td>md5</td><td>md5</td></tr><tr><td>sha1</td><td>sha1</td></tr><tr><td>sha256</td><td>sha256</td></tr><tr><td>sha384</td><td>sha384</td></tr><tr><td>sha512</td><td>sha512</td></tr></table>	Option	Description	null	null	md5	md5	sha1	sha1	sha256	sha256	sha384	sha384	sha512	sha512											
	Option	Description																								
	null	null																								
	md5	md5																								
	sha1	sha1																								
	sha256	sha256																								
	sha384	sha384																								
sha512	sha512																									
auth-key	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																							
enc-alg	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-	null																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>null</td><td>null</td></tr><tr><td>des</td><td>des</td></tr><tr><td>3des</td><td>3des</td></tr><tr><td>aes128</td><td>aes128</td></tr><tr><td>aes192</td><td>aes192</td></tr><tr><td>aes256</td><td>aes256</td></tr><tr><td>aria128</td><td>aria128</td></tr><tr><td>aria192</td><td>aria192</td></tr><tr><td>aria256</td><td>aria256</td></tr><tr><td>seed</td><td>seed</td></tr></table>	Option	Description	null	null	des	des	3des	3des	aes128	aes128	aes192	aes192	aes256	aes256	aria128	aria128	aria192	aria192	aria256	aria256	seed	seed			
	Option	Description																								
	null	null																								
	des	des																								
	3des	3des																								
	aes128	aes128																								
	aes192	aes192																								
	aes256	aes256																								
	aria128	aria128																								
	aria192	aria192																								
aria256	aria256																									
seed	seed																									
enc-key	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																							
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15																							

Parameter	Description	Type	Size	Default						
ip-version	IP version to use for VPN interface.	option	-	4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for gateways.</td></tr><tr><td>6</td><td>Use IPv6 addressing for gateways.</td></tr></table>				Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.
	Option	Description								
	4	Use IPv4 addressing for gateways.								
6	Use IPv6 addressing for gateways.									
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address-any	Not Specified	0.0.0.0						
local-gw6	Local IPv6 address of VPN gateway.	ipv6-address	Not Specified	::						
local-spi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified							
name	IPsec tunnel name.	string	Maximum length: 15							
npu-offload *	Enable/disable offloading IPsec VPN manual key sessions to NPUs.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NPU offloading.</td></tr><tr><td>disable</td><td>Disable NPU offloading.</td></tr></table>				Option	Description	enable	Enable NPU offloading.	disable	Disable NPU offloading.
	Option	Description								
	enable	Enable NPU offloading.								
disable	Disable NPU offloading.									
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0						
remote-gw6	Remote IPv6 address of VPN gateway.	ipv6-address	Not Specified	::						
remote-spi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified							

* This parameter may not exist in some models.

config vpn ipsec phase1

Configure VPN remote gateway.

```
config vpn ipsec phase1
  Description: Configure VPN remote gateway.
  edit <name>
    set acct-verify [enable|disable]
    set add-gw-route [enable|disable]
```

```

set add-route [disable|enable]
set addke1 {option1}, {option2}, ...
set addke2 {option1}, {option2}, ...
set addke3 {option1}, {option2}, ...
set addke4 {option1}, {option2}, ...
set addke5 {option1}, {option2}, ...
set addke6 {option1}, {option2}, ...
set addke7 {option1}, {option2}, ...
set assign-ip [disable|enable]
set assign-ip-from [range|usrgrp|...]
set authmethod [psk|signature]
set authmethod-remote [psk|signature]
set authpasswd {password}
set authusr {string}
set authusrgrp {string}
set auto-negotiate [enable|disable]
set auto-transport-threshold {integer}
set azure-ad-autoconnect [enable|disable]
set backup-gateway <address1>, <address2>, ...
set banner {var-string}
set cert-id-validation [enable|disable]
set cert-peer-username-strip [disable|enable]
set cert-peer-username-validation [none|othername|...]
set cert-trust-store [local|ems]
set certificate <name1>, <name2>, ...
set childless-ike [enable|disable]
set client-auto-negotiate [disable|enable]
set client-keep-alive [disable|enable]
set client-resume [enable|disable]
set client-resume-interval {integer}
set comments {var-string}
set dev-id {string}
set dev-id-notification [disable|enable]
set dhcp-ra-giaddr {ipv4-address}
set dhcp6-ra-linkaddr {ipv6-address}
set dhgrp {option1}, {option2}, ...
set digital-signature-auth [enable|disable]
set distance {integer}
set dns-mode [manual|auto]
set domain {string}
set dpd [disable|on-idle|...]
set dpd-retrycount {integer}
set dpd-retryinterval {user}
set eap [enable|disable]
set eap-cert-auth [enable|disable]
set eap-exclude-peergrp {string}
set eap-identity [use-id-payload|send-request]
set ems-sn-check [enable|disable]
set enforce-unique-id [disable|keep-new|...]
set esn [require|allow|...]
set exchange-fgt-device-id [enable|disable]
set fec-base {integer}

```

```

set fec-codec [rs|xor]
set fec-egress [enable|disable]
set fec-health-check {string}
set fec-ingress [enable|disable]
set fec-mapping-profile {string}
set fec-receive-timeout {integer}
set fec-redundant {integer}
set fec-send-timeout {integer}
set fgsp-sync [enable|disable]
set fortinet-esp [enable|disable]
set fragmentation [enable|disable]
set fragmentation-mtu {integer}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set ha-sync-esp-seqno [enable|disable]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ike-version [1|2]
set inbound-dscp-copy [enable|disable]
set include-local-lan [disable|enable]
set interface {string}
set internal-domain-list <domain-name1>, <domain-name2>, ...
set ip-delay-interval {integer}
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-end-ip {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set end-ip {ipv4-address}
        set start-ip {ipv4-address}
    next
end
set ipv4-name {string}
set ipv4-netmask {ipv4-netmask}
set ipv4-split-exclude {string}
set ipv4-split-include {string}
set ipv4-start-ip {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
set ipv6-auto-linklocal [enable|disable]
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
set ipv6-end-ip {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set end-ip {ipv6-address}
        set start-ip {ipv6-address}
    next

```

```

end
set ipv6-name {string}
set ipv6-prefix {integer}
set ipv6-split-exclude {string}
set ipv6-split-include {string}
set ipv6-start-ip {ipv6-address}
set keepalive {integer}
set keylife {integer}
set kms {string}
set link-cost {integer}
set local-gw {ipv4-address}
set localid {string}
set localid-type [auto|fqdn|...]
set loopback-asymroute [enable|disable]
set mesh-selector-type [disable|subnet|...]
set mode [aggressive|main]
set mode-cfg [disable|enable]
set mode-cfg-allow-client-selector [disable|enable]
set nattraversal [enable|disable|...]
set negotiate-timeout {integer}
set network-id {integer}
set network-overlay [disable|enable]
set npu-offload [enable|disable]
set peer {string}
set peergrp {string}
set peerid {string}
set peertype [any|one|...]
set ppk [disable|allow|...]
set ppk-identity {string}
set ppk-secret {password-3}
set priority {integer}
set proposal {option1}, {option2}, ...
set psksecret {password-3}
set psksecret-remote {password-3}
set qkd [disable|allow|...]
set qkd-hybrid [disable|allow|...]
set qkd-profile {string}
set reauth [disable|enable]
set rekey [enable|disable]
set remote-gw {ipv4-address}
set remote-gw-country {string}
set remote-gw-end-ip {ipv4-address-any}
set remote-gw-match [any|ipmask|...]
set remote-gw-start-ip {ipv4-address-any}
set remote-gw-subnet {ipv4-classnet-any}
set remote-gw-ztna-tags <name1>, <name2>, ...
set remote-gw6-country {string}
set remote-gw6-end-ip {ipv6-address}
set remote-gw6-match [any|ipprefix|...]
set remote-gw6-start-ip {ipv6-address}
set remote-gw6-subnet {ipv6-network}
set remotegw-ddns {string}

```

```

set rsa-signature-format [pkcs1|pss]
set rsa-signature-hash-override [enable|disable]
set save-password [disable|enable]
set send-cert-chain [enable|disable]
set shared-idle-timeout [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set split-include-service {string}
set suite-b [disable|suite-b-gcm-128|...]
set transport [udp|auto|...]
set type [static|dynamic|...]
set unity-support [disable|enable]
set usrgrp {string}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]
next
end

```

config vpn ipsec phase1

Parameter	Description	Type	Size	Default
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable verification of RADIUS accounting record.		
	<i>disable</i>	Disable verification of RADIUS accounting record.		
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-	disable
	Option	Description		
	<i>enable</i>	Automatically add a route to the remote gateway.		
	<i>disable</i>	Do not automatically add a route to the remote gateway.		
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not add a route to destination of peer selector.		
	<i>enable</i>	Add route to destination of peer selector.		
addke1	ADDKE1 group.	option	-	

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					
addke2	ADDKE2 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.															
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
1085	FRODO L5.																																					

Parameter	Description	Type	Size	Default
	Option	Description		
	1089	BIKE L1.		
	1090	BIKE L3.		
	1091	BIKE L5.		
	1092	HQC128.		
	1093	HQC192.		
	1094	HQC256.		
addke3	ADDKE3 group.	option	-	
	Option	Description		
	0	NONE.		
	35	ML-KEM-512.		
	36	ML-KEM-768.		
	37	ML-KEM-1024.		
	1080	KYBER512.		
	1081	KYBER768.		
	1082	KYBER1024.		
	1083	FRODO L1.		
	1084	FRODO L3.		
	1085	FRODO L5.		
	1089	BIKE L1.		
	1090	BIKE L3.		
	1091	BIKE L5.		
	1092	HQC128.		
	1093	HQC192.		
	1094	HQC256.		
addke4	ADDKE4 group.	option	-	
	Option	Description		
	0	NONE.		
	35	ML-KEM-512.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																
	36	ML-KEM-768.																																
	37	ML-KEM-1024.																																
	1080	KYBER512.																																
	1081	KYBER768.																																
	1082	KYBER1024.																																
	1083	FRODO L1.																																
	1084	FRODO L3.																																
	1085	FRODO L5.																																
	1089	BIKE L1.																																
	1090	BIKE L3.																																
	1091	BIKE L5.																																
	1092	HQC128.																																
	1093	HQC192.																																
	1094	HQC256.																																
addke5	ADDKE5 group.	option	-																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.							
	Option	Description																																
	0	NONE.																																
	35	ML-KEM-512.																																
	36	ML-KEM-768.																																
	37	ML-KEM-1024.																																
	1080	KYBER512.																																
	1081	KYBER768.																																
	1082	KYBER1024.																																
	1083	FRODO L1.																																
	1084	FRODO L3.																																
	1085	FRODO L5.																																
	1089	BIKE L1.																																
	1090	BIKE L3.																																

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.																											
	Option	Description																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
	1094	HQC256.																																				
addke6	ADDKE6 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
	1094	HQC256.																																				
	addke7	ADDKE7 group.	option	-																																		
		<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.																										
Option		Description																																				
0		NONE.																																				
35		ML-KEM-512.																																				
36		ML-KEM-768.																																				
37		ML-KEM-1024.																																				

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																												
	1080	KYBER512.																												
	1081	KYBER768.																												
	1082	KYBER1024.																												
	1083	FRODO L1.																												
	1084	FRODO L3.																												
	1085	FRODO L5.																												
	1089	BIKE L1.																												
	1090	BIKE L3.																												
	1091	BIKE L5.																												
	1092	HQC128.																												
	1093	HQC192.																												
	1094	HQC256.																												
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-	enable																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not assign an IP address to the IPsec interface.</td></tr><tr><td>enable</td><td>Assign an IP address to the IPsec interface.</td></tr></table>	Option	Description	disable	Do not assign an IP address to the IPsec interface.	enable	Assign an IP address to the IPsec interface.																							
	Option	Description																												
	disable	Do not assign an IP address to the IPsec interface.																												
enable	Assign an IP address to the IPsec interface.																													
assign-ip-from	Method by which the IP address will be assigned.	option	-	range																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>range</td><td>Assign IP address from locally defined range.</td></tr><tr><td>usrgrp</td><td>Assign IP address via user group.</td></tr><tr><td>dhcp</td><td>Assign IP address via DHCP.</td></tr><tr><td>name</td><td>Assign IP address from firewall address or group.</td></tr></table>	Option	Description	range	Assign IP address from locally defined range.	usrgrp	Assign IP address via user group.	dhcp	Assign IP address via DHCP.	name	Assign IP address from firewall address or group.																			
	Option	Description																												
	range	Assign IP address from locally defined range.																												
	usrgrp	Assign IP address via user group.																												
	dhcp	Assign IP address via DHCP.																												
name	Assign IP address from firewall address or group.																													
authmethod	Authentication method.	option	-	psk																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>psk</td><td>PSK authentication method.</td></tr><tr><td>signature</td><td>Signature authentication method.</td></tr></table>	Option	Description	psk	PSK authentication method.	signature	Signature authentication method.																							
	Option	Description																												
	psk	PSK authentication method.																												
signature	Signature authentication method.																													

Parameter	Description	Type	Size	Default						
authmethod-remote	Authentication method (remote side).	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>psk</i></td><td>PSK authentication method.</td></tr><tr><td><i>signature</i></td><td>Signature authentication method.</td></tr></table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.			
Option	Description									
<i>psk</i>	PSK authentication method.									
<i>signature</i>	Signature authentication method.									
authpasswd	XAuth password (max 35 characters).	password	Not Specified							
authusr	XAuth user name.	string	Maximum length: 64							
authusrgrp	Authentication user group.	string	Maximum length: 35							
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic initiation of IKE SA negotiation.</td></tr><tr><td><i>disable</i></td><td>Disable automatic initiation of IKE SA negotiation.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.			
Option	Description									
<i>enable</i>	Enable automatic initiation of IKE SA negotiation.									
<i>disable</i>	Disable automatic initiation of IKE SA negotiation.									
auto-transport-threshold	Timeout in seconds before falling back to next transport protocol.	integer	Minimum value: 1 Maximum value: 300	15						
azure-ad-autoconnect	Enable/disable Azure AD Auto-Connect for FortiClient.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Azure AD Auto-Connect for FortiClient.</td></tr><tr><td><i>disable</i></td><td>Disable Azure AD Auto-Connect for FortiClient.</td></tr></table>	Option	Description	<i>enable</i>	Enable Azure AD Auto-Connect for FortiClient.	<i>disable</i>	Disable Azure AD Auto-Connect for FortiClient.			
Option	Description									
<i>enable</i>	Enable Azure AD Auto-Connect for FortiClient.									
<i>disable</i>	Disable Azure AD Auto-Connect for FortiClient.									
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79							
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024							
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.		
	<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.		
cert-peer-username-strip	Enable/disable domain stripping on certificate identity.	option	-	disable
	Option Description			
	<i>disable</i>	Disable domain stripping on certificate identity.		
	<i>enable</i>	Enable domain stripping on certificate identity.		
cert-peer-username-validation	Enable/disable cross validation of peer username and the identity in the peer's certificate.	option	-	none
	Option Description			
	<i>none</i>	Disable cross validation of peer username and the identity in the peer's certificate.		
	<i>othername</i>	Validate principal name in SAN othername.		
	<i>rfc822name</i>	Validate RFC822 email address in SAN.		
	<i>cn</i>	Validate CN in subject.		
cert-trust-store	CA certificate trust store.	option	-	local
	Option Description			
	<i>local</i>	Use local CA certificate.		
	<i>ems</i>	Use EMS CA certificate.		
certificate <name>	Names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79	
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable
	Option Description			
	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).		
	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).		

Parameter	Description	Type	Size	Default						
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable allowing the VPN client to bring up the tunnel when there is no traffic.</td></tr><tr><td>enable</td><td>Enable allowing the VPN client to bring up the tunnel when there is no traffic.</td></tr></table>	Option	Description	disable	Disable allowing the VPN client to bring up the tunnel when there is no traffic.	enable	Enable allowing the VPN client to bring up the tunnel when there is no traffic.			
Option	Description									
disable	Disable allowing the VPN client to bring up the tunnel when there is no traffic.									
enable	Enable allowing the VPN client to bring up the tunnel when there is no traffic.									
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable allowing the VPN client to keep the tunnel up when there is no traffic.</td></tr><tr><td>enable</td><td>Enable allowing the VPN client to keep the tunnel up when there is no traffic.</td></tr></table>	Option	Description	disable	Disable allowing the VPN client to keep the tunnel up when there is no traffic.	enable	Enable allowing the VPN client to keep the tunnel up when there is no traffic.			
Option	Description									
disable	Disable allowing the VPN client to keep the tunnel up when there is no traffic.									
enable	Enable allowing the VPN client to keep the tunnel up when there is no traffic.									
client-resume	Enable/disable resumption of offline FortiClient sessions. When a FortiClient enabled laptop is closed or enters sleep/hibernate mode, enabling this feature allows FortiClient to keep the tunnel during this period, and allows users to immediately resume using the IPsec tunnel when the device wakes up.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable client session resumption.</td></tr><tr><td>disable</td><td>Disable client session resumption.</td></tr></table>	Option	Description	enable	Enable client session resumption.	disable	Disable client session resumption.			
Option	Description									
enable	Enable client session resumption.									
disable	Disable client session resumption.									
client-resume-interval	Maximum time in seconds during which a VPN client may resume using a tunnel after a client PC has entered sleep mode or temporarily lost its network connection (120 - 172800, default = 7200).	integer	Minimum value: 120 Maximum value: 172800	7200						
comments	Comment.	var-string	Maximum length: 255							

Parameter	Description	Type	Size	Default
dev-id	Device ID carried by the device ID notification.	string	Maximum length: 63	
dev-id-notification	Enable/disable device ID notification.	option	-	disable
	Option		Description	
	disable		Disable device ID notification.	
	enable		Enable device ID notification.	
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified	0.0.0.0
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified	::
dhgrp	DH group.	option	-	14
	Option		Description	
	1		DH Group 1.	
	2		DH Group 2.	
	5		DH Group 5.	
	14		DH Group 14.	
	15		DH Group 15.	
	16		DH Group 16.	
	17		DH Group 17.	
	18		DH Group 18.	
	19		DH Group 19.	
	20		DH Group 20.	
	21		DH Group 21.	
	27		DH Group 27.	
	28		DH Group 28.	
	29		DH Group 29.	
	30		DH Group 30.	
	31		DH Group 31.	
	32		DH Group 32.	

Parameter	Description	Type	Size	Default								
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr><tr><td>disable</td><td>Disable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr></table>	Option	Description	enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).	disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).					
Option	Description											
enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).											
disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).											
distance	Distance for routes added by IKE (1 - 255).	integer	Minimum value: 1 Maximum value: 255	15								
dns-mode	DNS server mode.	option	-	manual								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>manual</td><td>Manually configure DNS servers.</td></tr><tr><td>auto</td><td>Use default DNS servers.</td></tr></table>	Option	Description	manual	Manually configure DNS servers.	auto	Use default DNS servers.					
Option	Description											
manual	Manually configure DNS servers.											
auto	Use default DNS servers.											
domain	Instruct unity clients about the single default DNS domain.	string	Maximum length: 63									
dpd	Dead Peer Detection mode.	option	-	on-demand								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Dead Peer Detection.</td></tr><tr><td>on-idle</td><td>Trigger Dead Peer Detection when IPsec is idle.</td></tr><tr><td>on-demand</td><td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td></tr></table>	Option	Description	disable	Disable Dead Peer Detection.	on-idle	Trigger Dead Peer Detection when IPsec is idle.	on-demand	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.			
Option	Description											
disable	Disable Dead Peer Detection.											
on-idle	Trigger Dead Peer Detection when IPsec is idle.											
on-demand	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.											
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3								
dpd-retryinterval	DPD retry interval.	user	Not Specified									
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IKEv2 EAP authentication.</td></tr><tr><td>disable</td><td>Disable IKEv2 EAP authentication.</td></tr></table>	Option	Description	enable	Enable IKEv2 EAP authentication.	disable	Disable IKEv2 EAP authentication.					
Option	Description											
enable	Enable IKEv2 EAP authentication.											
disable	Disable IKEv2 EAP authentication.											

Parameter	Description	Type	Size	Default								
eap-cert-auth	Enable/disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.</td></tr><tr><td><i>disable</i></td><td>Disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.</td></tr></table>	Option	Description	<i>enable</i>	Enable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.	<i>disable</i>	Disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.					
Option	Description											
<i>enable</i>	Enable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.											
<i>disable</i>	Disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.											
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35									
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-id-payload</i></td><td>Use IKEv2 IDi payload to resolve peer identity.</td></tr><tr><td><i>send-request</i></td><td>Use EAP identity request to resolve peer identity.</td></tr></table>	Option	Description	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.	<i>send-request</i>	Use EAP identity request to resolve peer identity.					
Option	Description											
<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.											
<i>send-request</i>	Use EAP identity request to resolve peer identity.											
ems-sn-check	Enable/disable verification of EMS serial number.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EMS serial number verification.</td></tr><tr><td><i>disable</i></td><td>Disable EMS serial number verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable EMS serial number verification.	<i>disable</i>	Disable EMS serial number verification.					
Option	Description											
<i>enable</i>	Enable EMS serial number verification.											
<i>disable</i>	Disable EMS serial number verification.											
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable peer ID uniqueness enforcement.</td></tr><tr><td><i>keep-new</i></td><td>Enforce peer ID uniqueness, keep new connection if collision found.</td></tr><tr><td><i>keep-old</i></td><td>Enforce peer ID uniqueness, keep old connection if collision found.</td></tr></table>	Option	Description	<i>disable</i>	Disable peer ID uniqueness enforcement.	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.	<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.			
Option	Description											
<i>disable</i>	Disable peer ID uniqueness enforcement.											
<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.											
<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.											
esn *	Extended sequence number (ESN) negotiation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>require</i></td><td>Require extended sequence number.</td></tr><tr><td><i>allow</i></td><td>Allow extended sequence number.</td></tr><tr><td><i>disable</i></td><td>Disable extended sequence number.</td></tr></table>	Option	Description	<i>require</i>	Require extended sequence number.	<i>allow</i>	Allow extended sequence number.	<i>disable</i>	Disable extended sequence number.			
Option	Description											
<i>require</i>	Require extended sequence number.											
<i>allow</i>	Allow extended sequence number.											
<i>disable</i>	Disable extended sequence number.											

Parameter	Description	Type	Size	Default
exchange-fgt-device-id	Enable/disable device identifier exchange with peer FortiGate units for use of VPN monitor data by FortiManager.	option	-	disable
	Option Description			
	<i>enable</i>	Enable exchange of FortiGate device identifier.		
	<i>disable</i>	Disable exchange of FortiGate device identifier.		
fec-base	Number of base Forward Error Correction packets (1 - 20).	integer	Minimum value: 1 Maximum value: 20	10
fec-codec	Forward Error Correction encoding/decoding algorithm.	option	-	rs
	Option Description			
	<i>rs</i>	Reed-Solomon FEC algorithm.		
	<i>xor</i>	XOR FEC algorithm.		
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-	disable
	Option Description			
	<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.		
	<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.		
fec-health-check	SD-WAN health check.	string	Maximum length: 35	
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-	disable
	Option Description			
	<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.		
	<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.		
fec-mapping-profile	Forward Error Correction (FEC) mapping profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets (1 - 1000).	integer	Minimum value: 1 Maximum value: 1000	50
fec-redundant	Number of redundant Forward Error Correction packets (1 - 5 for reed-solomon, 1 for xor).	integer	Minimum value: 1 Maximum value: 5	1
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets (1 - 1000).	integer	Minimum value: 1 Maximum value: 1000	5
fgsp-sync	Enable/disable IPsec syncing of tunnels for FGSP IPsec.	option	-	disable
	Option	Description		
	enable	Enable IPsec syncing of tunnels to other cluster members.		
	disable	Disable IPsec syncing of tunnels to other cluster members.		
fortinet-esp	Enable/disable Fortinet ESP encapsulaton.	option	-	disable
	Option	Description		
	enable	Enable Fortinet ESP encapsulation.		
	disable	Disable Fortinet ESP encapsulaton.		
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable
	Option	Description		
	enable	Enable intra-IKE fragmentation support on re-transmission.		
	disable	Disable intra-IKE fragmentation support.		
fragmentation-mtu	IKE fragmentation MTU (500 - 16000).	integer	Minimum value: 500 Maximum value: 16000	1200
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable IKEv2 IDi group authentication.		
	<i>disable</i>	Disable IKEv2 IDi group authentication.		
group-authentication-secret	Password for IKEv2 ID group authentication. ASCII string or hexadecimal indicated by a leading 0x.	password-3	Not Specified	
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-	enable
	Option Description			
	<i>enable</i>	Enable HA syncing of ESP sequence numbers.		
	<i>disable</i>	Disable HA syncing of ESP sequence numbers.		
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable
	Option Description			
	<i>enable</i>	Enable IPsec tunnel idle timeout.		
	<i>disable</i>	Disable IPsec tunnel idle timeout.		
idle-timeoutinterval	IPsec tunnel idle timeout in minutes (5 - 43200).	integer	Minimum value: 5 Maximum value: 43200	15
ike-version	IKE protocol version.	option	-	1
	Option Description			
	1	Use IKEv1 protocol.		
	2	Use IKEv2 protocol.		
inbound-dscp-copy	Enable/disable copy the dscp in the ESP header to the inner IP Header.	option	-	disable
	Option Description			
	<i>enable</i>	Enable copy the dscp in the ESP header to the inner IP Header.		
	<i>disable</i>	Disable copy the dscp in the ESP header to the inner IP Header.		

Parameter	Description	Type	Size	Default						
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable local LAN access on Unity clients.</td></tr><tr><td>enable</td><td>Enable local LAN access on Unity clients.</td></tr></table>	Option	Description	disable	Disable local LAN access on Unity clients.	enable	Enable local LAN access on Unity clients.			
Option	Description									
disable	Disable local LAN access on Unity clients.									
enable	Enable local LAN access on Unity clients.									
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35							
internal-domain-list <domain-name>	One or more internal domain names in quotes separated by spaces. Domain name.	string	Maximum length: 79							
ip-delay-interval	IP address reuse delay interval in seconds (0 - 28800).	integer	Minimum value: 0 Maximum value: 28800	0						
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0						
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0						
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified	0.0.0.0						
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0						
ipv4-name	IPv4 address name.	string	Maximum length: 79							
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified	255.255.255.255						
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79							
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79							
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0						
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0						
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default						
ipv6-auto-linklocal	Enable/disable auto generation of IPv6 link-local address using last 8 bytes of mode-cfg assigned IPv6 address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable mode-cfg auto configuration of IPv6 link-local address.</td></tr><tr><td>disable</td><td>Disable mode-cfg auto configuration of IPv6 link-local address.</td></tr></table>	Option	Description	enable	Enable mode-cfg auto configuration of IPv6 link-local address.	disable	Disable mode-cfg auto configuration of IPv6 link-local address.			
Option	Description									
enable	Enable mode-cfg auto configuration of IPv6 link-local address.									
disable	Disable mode-cfg auto configuration of IPv6 link-local address.									
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::						
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::						
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified	::						
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified	::						
ipv6-name	IPv6 address name.	string	Maximum length: 79							
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128	128						
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79							
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79							
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified	::						
keepalive	NAT-T keep alive interval.	integer	Minimum value: 5 Maximum value: 900	10						
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400						
kms	Key Management Services server.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
link-cost	VPN tunnel underlay link cost.	integer	Minimum value: 0 Maximum value: 255	0
local-gw	Local VPN gateway.	ipv4-address	Not Specified	0.0.0.0
localid	Local ID.	string	Maximum length: 63	
localid-type	Local ID type.	option	-	auto
	Option		Description	
	auto		Select ID type automatically.	
	fqdn		Use fully qualified domain name.	
	user-fqdn		Use user fully qualified domain name.	
	keyid		Use key-id string.	
	address		Use local IP address.	
	asn1dn		Use ASN.1 distinguished name.	
loopback-asymroute	Enable/disable asymmetric routing for IKE traffic on loopback interface.	option	-	enable
	Option		Description	
	enable		Allow ingress/egress IKE traffic to be routed over different interfaces.	
	disable		Ingress/egress IKE traffic must be routed over the same interface.	
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-	disable
	Option		Description	
	disable		Disable.	
	subnet		Enable addition of matching subnet selector.	
	host		Enable addition of host to host selector.	
mode	ID protection mode used to establish a secure channel.	option	-	main

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aggressive</i></td><td>Aggressive mode.</td></tr><tr><td><i>main</i></td><td>Main mode.</td></tr></table>	Option	Description	<i>aggressive</i>	Aggressive mode.	<i>main</i>	Main mode.					
	Option	Description										
	<i>aggressive</i>	Aggressive mode.										
<i>main</i>	Main mode.											
mode-cfg	Enable/disable configuration method.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Configuration Method.</td></tr><tr><td><i>enable</i></td><td>Enable Configuration Method.</td></tr></table>	Option	Description	<i>disable</i>	Disable Configuration Method.	<i>enable</i>	Enable Configuration Method.					
	Option	Description										
	<i>disable</i>	Disable Configuration Method.										
<i>enable</i>	Enable Configuration Method.											
mode-cfg-allow-client-selector	Enable/disable mode-cfg client to use custom phase2 selectors.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Mode-cfg client to use wildcard selectors.</td></tr><tr><td><i>enable</i></td><td>Mode-cfg client to use custom selectors.</td></tr></table>	Option	Description	<i>disable</i>	Mode-cfg client to use wildcard selectors.	<i>enable</i>	Mode-cfg client to use custom selectors.					
	Option	Description										
	<i>disable</i>	Mode-cfg client to use wildcard selectors.										
<i>enable</i>	Mode-cfg client to use custom selectors.											
name	IPsec remote gateway name.	string	Maximum length: 35									
nattraversal	Enable/disable NAT traversal.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec NAT traversal.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec NAT traversal.</td></tr><tr><td><i>forced</i></td><td>Force IPsec NAT traversal on.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec NAT traversal.	<i>disable</i>	Disable IPsec NAT traversal.	<i>forced</i>	Force IPsec NAT traversal on.			
	Option	Description										
	<i>enable</i>	Enable IPsec NAT traversal.										
	<i>disable</i>	Disable IPsec NAT traversal.										
<i>forced</i>	Force IPsec NAT traversal on.											
negotiate-timeout	IKE SA negotiation timeout in seconds (1 - 300).	integer	Minimum value: 1 Maximum value: 300	30								
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255	0								
network-overlay	Enable/disable network overlays.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable network overlays.</td></tr><tr><td><i>enable</i></td><td>Enable network overlays.</td></tr></table>	Option	Description	<i>disable</i>	Disable network overlays.	<i>enable</i>	Enable network overlays.					
	Option	Description										
	<i>disable</i>	Disable network overlays.										
<i>enable</i>	Enable network overlays.											

Parameter	Description	Type	Size	Default												
npu-offload *	Enable/disable offloading NPU.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU offloading.</td></tr><tr><td><i>disable</i></td><td>Disable NPU offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU offloading.	<i>disable</i>	Disable NPU offloading.									
Option	Description															
<i>enable</i>	Enable NPU offloading.															
<i>disable</i>	Disable NPU offloading.															
peer	Accept this peer certificate.	string	Maximum length: 35													
peergrp	Accept this peer certificate group.	string	Maximum length: 35													
peerid	Accept this peer identity.	string	Maximum length: 255													
peertype	Accept this peer type.	option	-	peer												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept any peer ID.</td></tr><tr><td><i>one</i></td><td>Accept this peer ID.</td></tr><tr><td><i>dialup</i></td><td>Accept peer ID in dialup group.</td></tr><tr><td><i>peer</i></td><td>Accept this peer certificate.</td></tr><tr><td><i>peergrp</i></td><td>Accept this peer certificate group.</td></tr></table>	Option	Description	<i>any</i>	Accept any peer ID.	<i>one</i>	Accept this peer ID.	<i>dialup</i>	Accept peer ID in dialup group.	<i>peer</i>	Accept this peer certificate.	<i>peergrp</i>	Accept this peer certificate group.			
Option	Description															
<i>any</i>	Accept any peer ID.															
<i>one</i>	Accept this peer ID.															
<i>dialup</i>	Accept peer ID in dialup group.															
<i>peer</i>	Accept this peer certificate.															
<i>peergrp</i>	Accept this peer certificate group.															
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>allow</i></td><td>Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>require</i></td><td>Require use of IKEv2 Postquantum Preshared Key (PPK).</td></tr></table>	Option	Description	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).							
Option	Description															
<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).															
<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).															
<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).															
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35													
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified													
priority	Priority for routes added by IKE (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	1												

Parameter	Description	Type	Size	Default
proposal	Phase1 proposal.	option	-	
	Option	Description		
	<i>des-md5</i>	des-md5		
	<i>des-sha1</i>	des-sha1		
	<i>des-sha256</i>	des-sha256		
	<i>des-sha384</i>	des-sha384		
	<i>des-sha512</i>	des-sha512		
	<i>3des-md5</i>	3des-md5		
	<i>3des-sha1</i>	3des-sha1		
	<i>3des-sha256</i>	3des-sha256		
	<i>3des-sha384</i>	3des-sha384		
	<i>3des-sha512</i>	3des-sha512		
	<i>aes128-md5</i>	aes128-md5		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1		
	<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256		
	<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384		
	<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1		
	<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256		
	<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384		
	<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512		
	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1		
	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256		
	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384		
	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		
	<i>aria128-sha512</i>	aria128-sha512		
	<i>aria192-md5</i>	aria192-md5		
	<i>aria192-sha1</i>	aria192-sha1		
	<i>aria192-sha256</i>	aria192-sha256		
	<i>aria192-sha384</i>	aria192-sha384		
	<i>aria192-sha512</i>	aria192-sha512		
	<i>aria256-md5</i>	aria256-md5		
	<i>aria256-sha1</i>	aria256-sha1		
	<i>aria256-sha256</i>	aria256-sha256		
	<i>aria256-sha384</i>	aria256-sha384		
	<i>aria256-sha512</i>	aria256-sha512		
	<i>seed-md5</i>	seed-md5		
	<i>seed-sha1</i>	seed-sha1		
	<i>seed-sha256</i>	seed-sha256		
	<i>seed-sha384</i>	seed-sha384		
	<i>seed-sha512</i>	seed-sha512		

Parameter	Description	Type	Size	Default								
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified									
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified									
qkd	Enable/disable use of Quantum Key Distribution (QKD) server.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of a Quantum Key Distribution (QKD) server.</td></tr><tr><td>allow</td><td>Allow, but do not require, use of a Quantum Key Distribution (QKD) server.</td></tr><tr><td>require</td><td>Require use of a Quantum Key Distribution (QKD) server.</td></tr></table>	Option	Description	disable	Disable use of a Quantum Key Distribution (QKD) server.	allow	Allow, but do not require, use of a Quantum Key Distribution (QKD) server.	require	Require use of a Quantum Key Distribution (QKD) server.			
Option	Description											
disable	Disable use of a Quantum Key Distribution (QKD) server.											
allow	Allow, but do not require, use of a Quantum Key Distribution (QKD) server.											
require	Require use of a Quantum Key Distribution (QKD) server.											
qkd-hybrid	Enable/disable use of Quantum Key Distribution (QKD) hybrid keys.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of Quantum Key Distribution (QKD) hybrid keys.</td></tr><tr><td>allow</td><td>Allow, but do not require, use of Quantum Key Distribution (QKD) hybrid keys.</td></tr><tr><td>require</td><td>Require use of Quantum Key Distribution (QKD) hybrid keys.</td></tr></table>	Option	Description	disable	Disable use of Quantum Key Distribution (QKD) hybrid keys.	allow	Allow, but do not require, use of Quantum Key Distribution (QKD) hybrid keys.	require	Require use of Quantum Key Distribution (QKD) hybrid keys.			
Option	Description											
disable	Disable use of Quantum Key Distribution (QKD) hybrid keys.											
allow	Allow, but do not require, use of Quantum Key Distribution (QKD) hybrid keys.											
require	Require use of Quantum Key Distribution (QKD) hybrid keys.											
qkd-profile	Quantum Key Distribution (QKD) server profile.	string	Maximum length: 35									
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable IKE SA re-authentication.</td></tr><tr><td>enable</td><td>Enable IKE SA re-authentication.</td></tr></table>	Option	Description	disable	Disable IKE SA re-authentication.	enable	Enable IKE SA re-authentication.					
Option	Description											
disable	Disable IKE SA re-authentication.											
enable	Enable IKE SA re-authentication.											
rekey	Enable/disable phase1 rekey.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable phase1 rekey.</td></tr><tr><td>disable</td><td>Disable phase1 rekey.</td></tr></table>	Option	Description	enable	Enable phase1 rekey.	disable	Disable phase1 rekey.					
Option	Description											
enable	Enable phase1 rekey.											
disable	Disable phase1 rekey.											

Parameter	Description	Type	Size	Default												
remote-gw	Remote VPN gateway.	ipv4-address	Not Specified	0.0.0.0												
remote-gw-country	IPv4 addresses associated to a specific country.	string	Maximum length: 2													
remote-gw-end-ip	Last IPv4 address in the range.	ipv4-address-any	Not Specified	0.0.0.0												
remote-gw-match	Set type of IPv4 remote gateway address matching.	option	-	any												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Match any IPv4 gateway address.</td></tr><tr><td><i>ipmask</i></td><td>Match IPv4 gateway address and mask.</td></tr><tr><td><i>iprange</i></td><td>Match IPv4 gateway address range.</td></tr><tr><td><i>geography</i></td><td>Match IPv4 gateway address from a specified country.</td></tr><tr><td><i>ztna</i></td><td>Match IPv4 gateway address against ZTNA posture tags.</td></tr></table>	Option	Description	<i>any</i>	Match any IPv4 gateway address.	<i>ipmask</i>	Match IPv4 gateway address and mask.	<i>iprange</i>	Match IPv4 gateway address range.	<i>geography</i>	Match IPv4 gateway address from a specified country.	<i>ztna</i>	Match IPv4 gateway address against ZTNA posture tags.			
Option	Description															
<i>any</i>	Match any IPv4 gateway address.															
<i>ipmask</i>	Match IPv4 gateway address and mask.															
<i>iprange</i>	Match IPv4 gateway address range.															
<i>geography</i>	Match IPv4 gateway address from a specified country.															
<i>ztna</i>	Match IPv4 gateway address against ZTNA posture tags.															
remote-gw-start-ip	First IPv4 address in the range.	ipv4-address-any	Not Specified	0.0.0.0												
remote-gw-subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0												
remote-gw-ztna-tags <name>	IPv4 ZTNA posture tags. Address name.	string	Maximum length: 79													
remote-gw6-country	IPv6 addresses associated to a specific country.	string	Maximum length: 2													
remote-gw6-end-ip	Last IPv6 address in the range.	ipv6-address	Not Specified	::												
remote-gw6-match	Set type of IPv6 remote gateway address matching.	option	-	any												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Match any IPv6 gateway address.</td></tr><tr><td><i>ipprefix</i></td><td>Match IPv6 gateway address and prefix.</td></tr><tr><td><i>iprange</i></td><td>Match IPv6 gateway address range.</td></tr><tr><td><i>geography</i></td><td>Match IPv6 gateway address from a specified country.</td></tr></table>	Option	Description	<i>any</i>	Match any IPv6 gateway address.	<i>ipprefix</i>	Match IPv6 gateway address and prefix.	<i>iprange</i>	Match IPv6 gateway address range.	<i>geography</i>	Match IPv6 gateway address from a specified country.					
Option	Description															
<i>any</i>	Match any IPv6 gateway address.															
<i>ipprefix</i>	Match IPv6 gateway address and prefix.															
<i>iprange</i>	Match IPv6 gateway address range.															
<i>geography</i>	Match IPv6 gateway address from a specified country.															
remote-gw6-start-ip	First IPv6 address in the range.	ipv6-address	Not Specified	::												

Parameter	Description	Type	Size	Default						
remote-gw6-subnet	IPv6 address and prefix.	ipv6-network	Not Specified	::/0						
remotegw-ddns	Domain name of remote gateway. For example, name.ddns.com.	string	Maximum length: 63							
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-	pkcs1						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pkcs1</td><td>RSASSA PKCS#1 v1.5.</td></tr><tr><td>pss</td><td>RSASSA Probabilistic Signature Scheme (PSS).</td></tr></table>	Option	Description	pkcs1	RSASSA PKCS#1 v1.5.	pss	RSASSA Probabilistic Signature Scheme (PSS).			
Option	Description									
pkcs1	RSASSA PKCS#1 v1.5.									
pss	RSASSA Probabilistic Signature Scheme (PSS).									
rsa-signature-hash-override	Enable/disable IKEv2 RSA signature hash algorithm override.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IKEv2 RSA signature hash algorithm override.</td></tr><tr><td>disable</td><td>Disable IKEv2 RSA signature hash algorithm override.</td></tr></table>	Option	Description	enable	Enable IKEv2 RSA signature hash algorithm override.	disable	Disable IKEv2 RSA signature hash algorithm override.			
Option	Description									
enable	Enable IKEv2 RSA signature hash algorithm override.									
disable	Disable IKEv2 RSA signature hash algorithm override.									
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable saving XAuth username and password on VPN clients.</td></tr><tr><td>enable</td><td>Enable saving XAuth username and password on VPN clients.</td></tr></table>	Option	Description	disable	Disable saving XAuth username and password on VPN clients.	enable	Enable saving XAuth username and password on VPN clients.			
Option	Description									
disable	Disable saving XAuth username and password on VPN clients.									
enable	Enable saving XAuth username and password on VPN clients.									
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending certificate chain.</td></tr><tr><td>disable</td><td>Disable sending certificate chain.</td></tr></table>	Option	Description	enable	Enable sending certificate chain.	disable	Disable sending certificate chain.			
Option	Description									
enable	Enable sending certificate chain.									
disable	Disable sending certificate chain.									
shared-idle-timeout	Enable/disable IPsec tunnel shared idle timeout.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPsec tunnel shared idle timeout. The location-id attribute must be configured on both spokes. Shared idle timeout is supported only on IKEv2 since remote-location is available only for IKEv2.</td></tr><tr><td>disable</td><td>Disable IPsec tunnel shared idle timeout.</td></tr></table>	Option	Description	enable	Enable IPsec tunnel shared idle timeout. The location-id attribute must be configured on both spokes. Shared idle timeout is supported only on IKEv2 since remote-location is available only for IKEv2.	disable	Disable IPsec tunnel shared idle timeout.			
Option	Description									
enable	Enable IPsec tunnel shared idle timeout. The location-id attribute must be configured on both spokes. Shared idle timeout is supported only on IKEv2 since remote-location is available only for IKEv2.									
disable	Disable IPsec tunnel shared idle timeout.									

Parameter	Description	Type	Size	Default										
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha1</td><td>SHA1.</td></tr><tr><td>sha2-256</td><td>SHA2-256.</td></tr><tr><td>sha2-384</td><td>SHA2-384.</td></tr><tr><td>sha2-512</td><td>SHA2-512.</td></tr></table>	Option	Description	sha1	SHA1.	sha2-256	SHA2-256.	sha2-384	SHA2-384.	sha2-512	SHA2-512.			
Option	Description													
sha1	SHA1.													
sha2-256	SHA2-256.													
sha2-384	SHA2-384.													
sha2-512	SHA2-512.													
split-include-service	Split-include services.	string	Maximum length: 79											
suite-b	Use Suite-B.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not use UI suite.</td></tr><tr><td>suite-b-gcm-128</td><td>Use Suite-B-GCM-128.</td></tr><tr><td>suite-b-gcm-256</td><td>Use Suite-B-GCM-256.</td></tr></table>	Option	Description	disable	Do not use UI suite.	suite-b-gcm-128	Use Suite-B-GCM-128.	suite-b-gcm-256	Use Suite-B-GCM-256.					
Option	Description													
disable	Do not use UI suite.													
suite-b-gcm-128	Use Suite-B-GCM-128.													
suite-b-gcm-256	Use Suite-B-GCM-256.													
transport	Set IKE transport protocol.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Use UDP transport for IKE.</td></tr><tr><td>auto</td><td>Use AUTO transport for IKE.</td></tr><tr><td>tcp</td><td>Use TCP transport for IKE.</td></tr></table>	Option	Description	udp	Use UDP transport for IKE.	auto	Use AUTO transport for IKE.	tcp	Use TCP transport for IKE.					
Option	Description													
udp	Use UDP transport for IKE.													
auto	Use AUTO transport for IKE.													
tcp	Use TCP transport for IKE.													
type	Remote gateway type.	option	-	static										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Remote VPN gateway has fixed IP address.</td></tr><tr><td>dynamic</td><td>Remote VPN gateway has dynamic IP address.</td></tr><tr><td>ddns</td><td>Remote VPN gateway has dynamic IP address and is a dynamic DNS client.</td></tr></table>	Option	Description	static	Remote VPN gateway has fixed IP address.	dynamic	Remote VPN gateway has dynamic IP address.	ddns	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.					
Option	Description													
static	Remote VPN gateway has fixed IP address.													
dynamic	Remote VPN gateway has dynamic IP address.													
ddns	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.													
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-	enable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.		
	<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.		
usrgrp	User group name for dialup peers.	string	Maximum length: 35	
wizard-type	GUI VPN Wizard Type.	option	-	custom
	Option	Description		
	<i>custom</i>	Custom VPN configuration.		
	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.		
	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.		
	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.		
	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.		
	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.		
	<i>static-fortigate</i>	Site to Site - FortiGate.		
	<i>dialup-fortigate</i>	Dial Up - FortiGate.		
	<i>static-cisco</i>	Site to Site - Cisco.		
	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.		
	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).		
	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.		
	<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.		
	<i>fabric-overlay-orchestrator</i>	Fabric Overlay Orchestrator.		
xauthtype	XAuth type.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>client</i>	Enable as client.		
	<i>pap</i>	Enable as server PAP.		
	<i>chap</i>	Enable as server CHAP.		
	<i>auto</i>	Enable as server auto.		

* This parameter may not exist in some models.

config ipv4-exclude-range

Parameter	Description	Type	Size	Default
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0

config ipv6-exclude-range

Parameter	Description	Type	Size	Default
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified	::
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified	::

config vpn ipsec phase1-interface

Configure VPN remote gateway.

```

config vpn ipsec phase1-interface
    Description: Configure VPN remote gateway.
    edit <name>
        set acct-verify [enable|disable]
        set add-gw-route [enable|disable]
        set add-route [disable|enable]
        set addke1 {option1}, {option2}, ...
        set addke2 {option1}, {option2}, ...
        set addke3 {option1}, {option2}, ...
        set addke4 {option1}, {option2}, ...
        set addke5 {option1}, {option2}, ...
        set addke6 {option1}, {option2}, ...
        set addke7 {option1}, {option2}, ...
        set aggregate-member [enable|disable]
        set aggregate-weight {integer}
        set assign-ip [disable|enable]
        set assign-ip-from [range|usrgrp|...]
        set authmethod [psk|signature]
        set authmethod-remote [psk|signature]
        set authpasswd {password}
        set authusr {string}
        set authusrgrp {string}
        set auto-discovery-crossover [allow|block]
        set auto-discovery-dialup-placeholder [disable|enable]
        set auto-discovery-forwarder [enable|disable]
        set auto-discovery-offer-interval {integer}
        set auto-discovery-psk [enable|disable]
        set auto-discovery-receiver [enable|disable]
        set auto-discovery-sender [enable|disable]
        set auto-discovery-shortcuts [independent|dependent]
        set auto-negotiate [enable|disable]
        set auto-transport-threshold {integer}
        set azure-ad-autoconnect [enable|disable]
        set backup-gateway <address1>, <address2>, ...
        set banner {var-string}
        set cert-id-validation [enable|disable]
        set cert-peer-username-strip [disable|enable]
        set cert-peer-username-validation [none|othername|...]
        set cert-trust-store [local|ems]
        set certificate <name1>, <name2>, ...
        set childless-ike [enable|disable]
        set client-auto-negotiate [disable|enable]
        set client-keep-alive [disable|enable]
        set client-resume [enable|disable]
        set client-resume-interval {integer}
        set comments {var-string}
        set default-gw {ipv4-address}
        set default-gw-priority {integer}
        set dev-id {string}
        set dev-id-notification [disable|enable]
        set dhcp-ra-giaddr {ipv4-address}
        set dhcp6-ra-linkaddr {ipv6-address}

```

```

set dhgrp {option1}, {option2}, ...
set digital-signature-auth [enable|disable]
set distance {integer}
set dns-mode [manual|auto]
set domain {string}
set dpd [disable|on-idle|...]
set dpd-retrycount {integer}
set dpd-retryinterval {user}
set eap [enable|disable]
set eap-cert-auth [enable|disable]
set eap-exclude-peergrp {string}
set eap-identity [use-id-payload|send-request]
set ems-sn-check [enable|disable]
set encap-local-gw4 {ipv4-address}
set encap-local-gw6 {ipv6-address}
set encap-remote-gw4 {ipv4-address}
set encap-remote-gw6 {ipv6-address}
set encapsulation [none|gre|...]
set encapsulation-address [ike|ipv4|...]
set enforce-unique-id [disable|keep-new|...]
set esn [require|allow|...]
set exchange-fgt-device-id [enable|disable]
set exchange-interface-ip [enable|disable]
set exchange-ip-addr4 {ipv4-address}
set exchange-ip-addr6 {ipv6-address}
set fec-base {integer}
set fec-codec [rs|xor]
set fec-egress [enable|disable]
set fec-health-check {string}
set fec-ingress [enable|disable]
set fec-mapping-profile {string}
set fec-receive-timeout {integer}
set fec-redundant {integer}
set fec-send-timeout {integer}
set fgsp-sync [enable|disable]
set fortinet-esp [enable|disable]
set fragmentation [enable|disable]
set fragmentation-mtu {integer}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set ha-sync-esp-seqno [enable|disable]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ike-version [1|2]
set inbound-dscp-copy [enable|disable]
set include-local-lan [disable|enable]
set interface {string}
set internal-domain-list <domain-name1>, <domain-name2>, ...
set ip-delay-interval {integer}
set ip-fragmentation [pre-encapsulation|post-encapsulation]
set ip-version [4|6]
set ipv4-dns-server1 {ipv4-address}

```

```

set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-end-ip {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set end-ip {ipv4-address}
        set start-ip {ipv4-address}
    next
end
set ipv4-name {string}
set ipv4-netmask {ipv4-netmask}
set ipv4-split-exclude {string}
set ipv4-split-include {string}
set ipv4-start-ip {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
set ipv6-auto-linklocal [enable|disable]
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
set ipv6-end-ip {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set end-ip {ipv6-address}
        set start-ip {ipv6-address}
    next
end
set ipv6-name {string}
set ipv6-prefix {integer}
set ipv6-split-exclude {string}
set ipv6-split-include {string}
set ipv6-start-ip {ipv6-address}
set keepalive {integer}
set keylife {integer}
set kms {string}
set link-cost {integer}
set local-gw {ipv4-address}
set local-gw6 {ipv6-address}
set localid {string}
set localid-type [auto|fqdn|...]
set loopback-asymroute [enable|disable]
set mesh-selector-type [disable|subnet|...]
set mode [aggressive|main]
set mode-cfg [disable|enable]
set mode-cfg-allow-client-selector [disable|enable]
set monitor <name1>, <name2>, ...
set monitor-hold-down-delay {integer}
set monitor-hold-down-time {user}
set monitor-hold-down-type [immediate|delay|...]
set monitor-hold-down-weekday [everyday|sunday|...]

```

```

set monitor-min {integer}
set natTraversal [enable|disable|...]
set negotiate-timeout {integer}
set net-device [enable|disable]
set network-id {integer}
set network-overlay [disable|enable]
set npu-offload [enable|disable]
set packet-redistribution [enable|disable]
set passive-mode [enable|disable]
set peer {string}
set peergrp {string}
set peerid {string}
set peertype [any|one|...]
set ppk [disable|allow|...]
set ppk-identity {string}
set ppk-secret {password-3}
set priority {integer}
set proposal {option1}, {option2}, ...
set psksecret {password-3}
set psksecret-remote {password-3}
set qkd [disable|allow|...]
set qkd-hybrid [disable|allow|...]
set qkd-profile {string}
set reauth [disable|enable]
set rekey [enable|disable]
set remote-gw {ipv4-address}
set remote-gw-country {string}
set remote-gw-end-ip {ipv4-address-any}
set remote-gw-match [any|ipmask|...]
set remote-gw-start-ip {ipv4-address-any}
set remote-gw-subnet {ipv4-classnet-any}
set remote-gw-ztna-tags <name1>, <name2>, ...
set remote-gw6 {ipv6-address}
set remote-gw6-country {string}
set remote-gw6-end-ip {ipv6-address}
set remote-gw6-match [any|ipprefix|...]
set remote-gw6-start-ip {ipv6-address}
set remote-gw6-subnet {ipv6-network}
set remotegw-ddns {string}
set rsa-signature-format [pkcs1|pss]
set rsa-signature-hash-override [enable|disable]
set save-password [disable|enable]
set send-cert-chain [enable|disable]
set shared-idle-timeout [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set split-include-service {string}
set suite-b [disable|suite-b-gcm-128|...]
set transport [udp|auto|...]
set type [static|dynamic|...]
set unity-support [disable|enable]
set usrgrp {string}
set vni {integer}

```

```

        set wizard-type [custom|dialup-forticlient|...]
        set xauthtype [disable|client|...]
    next
end

```

config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable verification of RADIUS accounting record.		
	<i>disable</i>	Disable verification of RADIUS accounting record.		
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-	disable
	Option	Description		
	<i>enable</i>	Automatically add a route to the remote gateway.		
	<i>disable</i>	Do not automatically add a route to the remote gateway.		
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	enable
	Option	Description		
	<i>disable</i>	Do not add a route to destination of peer selector.		
	<i>enable</i>	Add route to destination of peer selector.		
addke1	ADDKE1 group.	option	-	
	Option	Description		
	<i>0</i>	NONE.		
	<i>35</i>	ML-KEM-512.		
	<i>36</i>	ML-KEM-768.		
	<i>37</i>	ML-KEM-1024.		
	<i>1080</i>	KYBER512.		
	<i>1081</i>	KYBER768.		
	<i>1082</i>	KYBER1024.		

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.																	
	Option	Description																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					
addke2	ADDKE2 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					
addke3	ADDKE3 group.	option	-																																			

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					
addke4	ADDKE4 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.															
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
1085	FRODO L5.																																					

Parameter	Description	Type	Size	Default
	Option	Description		
	1089	BIKE L1.		
	1090	BIKE L3.		
	1091	BIKE L5.		
	1092	HQC128.		
	1093	HQC192.		
	1094	HQC256.		
addke5	ADDKE5 group.	option	-	
	Option	Description		
	0	NONE.		
	35	ML-KEM-512.		
	36	ML-KEM-768.		
	37	ML-KEM-1024.		
	1080	KYBER512.		
	1081	KYBER768.		
	1082	KYBER1024.		
	1083	FRODO L1.		
	1084	FRODO L3.		
	1085	FRODO L5.		
	1089	BIKE L1.		
	1090	BIKE L3.		
	1091	BIKE L5.		
	1092	HQC128.		
	1093	HQC192.		
	1094	HQC256.		
addke6	ADDKE6 group.	option	-	
	Option	Description		
	0	NONE.		
	35	ML-KEM-512.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																
	36	ML-KEM-768.																																
	37	ML-KEM-1024.																																
	1080	KYBER512.																																
	1081	KYBER768.																																
	1082	KYBER1024.																																
	1083	FRODO L1.																																
	1084	FRODO L3.																																
	1085	FRODO L5.																																
	1089	BIKE L1.																																
	1090	BIKE L3.																																
	1091	BIKE L5.																																
	1092	HQC128.																																
	1093	HQC192.																																
	1094	HQC256.																																
addke7	ADDKE7 group.	option	-																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.							
	Option	Description																																
	0	NONE.																																
	35	ML-KEM-512.																																
	36	ML-KEM-768.																																
	37	ML-KEM-1024.																																
	1080	KYBER512.																																
	1081	KYBER768.																																
	1082	KYBER1024.																																
	1083	FRODO L1.																																
	1084	FRODO L3.																																
	1085	FRODO L5.																																
	1089	BIKE L1.																																
	1090	BIKE L3.																																

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description												
	1091	BIKE L5.												
	1092	HQC128.												
	1093	HQC192.												
1094	HQC256.													
aggregate-member	Enable/disable use as an aggregate member.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use as an aggregate member.</td></tr><tr><td>disable</td><td>Disable use as an aggregate member.</td></tr></table>	Option	Description	enable	Enable use as an aggregate member.	disable	Disable use as an aggregate member.							
	Option	Description												
	enable	Enable use as an aggregate member.												
disable	Disable use as an aggregate member.													
aggregate-weight	Link weight for aggregate.	integer	Minimum value: 1 1 Maximum value: 100											
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not assign an IP address to the IPsec interface.</td></tr><tr><td>enable</td><td>Assign an IP address to the IPsec interface.</td></tr></table>	Option	Description	disable	Do not assign an IP address to the IPsec interface.	enable	Assign an IP address to the IPsec interface.							
	Option	Description												
	disable	Do not assign an IP address to the IPsec interface.												
enable	Assign an IP address to the IPsec interface.													
assign-ip-from	Method by which the IP address will be assigned.	option	-	range										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>range</td><td>Assign IP address from locally defined range.</td></tr><tr><td>usrgrp</td><td>Assign IP address via user group.</td></tr><tr><td>dhcp</td><td>Assign IP address via DHCP.</td></tr><tr><td>name</td><td>Assign IP address from firewall address or group.</td></tr></table>	Option	Description	range	Assign IP address from locally defined range.	usrgrp	Assign IP address via user group.	dhcp	Assign IP address via DHCP.	name	Assign IP address from firewall address or group.			
	Option	Description												
	range	Assign IP address from locally defined range.												
	usrgrp	Assign IP address via user group.												
	dhcp	Assign IP address via DHCP.												
name	Assign IP address from firewall address or group.													
authmethod	Authentication method.	option	-	psk										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>psk</td><td>PSK authentication method.</td></tr><tr><td>signature</td><td>Signature authentication method.</td></tr></table>	Option	Description	psk	PSK authentication method.	signature	Signature authentication method.							
	Option	Description												
	psk	PSK authentication method.												
signature	Signature authentication method.													

Parameter	Description	Type	Size	Default						
authmethod-remote	Authentication method (remote side).	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>psk</i></td><td>PSK authentication method.</td></tr><tr><td><i>signature</i></td><td>Signature authentication method.</td></tr></table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.			
Option	Description									
<i>psk</i>	PSK authentication method.									
<i>signature</i>	Signature authentication method.									
authpasswd	XAuth password (max 35 characters).	password	Not Specified							
authusr	XAuth user name.	string	Maximum length: 64							
authusrgrp	Authentication user group.	string	Maximum length: 35							
auto-discovery-crossover	Allow/block set-up of short-cut tunnels between different network IDs.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow set-up of short-cut tunnels between different network IDs.</td></tr><tr><td><i>block</i></td><td>Block set-up of short-cut tunnels between different network IDs.</td></tr></table>	Option	Description	<i>allow</i>	Allow set-up of short-cut tunnels between different network IDs.	<i>block</i>	Block set-up of short-cut tunnels between different network IDs.			
Option	Description									
<i>allow</i>	Allow set-up of short-cut tunnels between different network IDs.									
<i>block</i>	Block set-up of short-cut tunnels between different network IDs.									
auto-discovery-dialup-placeholder	Control if this dynamic gateway is used for shortcut connections only.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable placeholder restriction.</td></tr><tr><td><i>enable</i></td><td>Enable placeholder restriction to only accept shortcut connections on this dial-up gateway.</td></tr></table>	Option	Description	<i>disable</i>	Disable placeholder restriction.	<i>enable</i>	Enable placeholder restriction to only accept shortcut connections on this dial-up gateway.			
Option	Description									
<i>disable</i>	Disable placeholder restriction.									
<i>enable</i>	Enable placeholder restriction to only accept shortcut connections on this dial-up gateway.									
auto-discovery-forwarder	Enable/disable forwarding auto-discovery short-cut messages.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forwarding auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable forwarding auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.			
Option	Description									
<i>enable</i>	Enable forwarding auto-discovery short-cut messages.									
<i>disable</i>	Disable forwarding auto-discovery short-cut messages.									
auto-discovery-offer-interval	Interval between shortcut offer messages in seconds (1 - 300, default = 5).	integer	Minimum value: 5 1 Maximum value: 300							

Parameter	Description	Type	Size	Default						
auto-discovery-psk	Enable/disable use of pre-shared secrets for authentication of auto-discovery tunnels.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of pre-shared-secret authentication for auto-discovery tunnels.</td></tr><tr><td><i>disable</i></td><td>Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of pre-shared-secret authentication for auto-discovery tunnels.	<i>disable</i>	Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.			
Option	Description									
<i>enable</i>	Enable use of pre-shared-secret authentication for auto-discovery tunnels.									
<i>disable</i>	Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.									
auto-discovery-receiver	Enable/disable accepting auto-discovery short-cut messages.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable receiving auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable receiving auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>enable</i>	Enable receiving auto-discovery short-cut messages.	<i>disable</i>	Disable receiving auto-discovery short-cut messages.			
Option	Description									
<i>enable</i>	Enable receiving auto-discovery short-cut messages.									
<i>disable</i>	Disable receiving auto-discovery short-cut messages.									
auto-discovery-sender	Enable/disable sending auto-discovery short-cut messages.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable sending auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending auto-discovery short-cut messages.	<i>disable</i>	Disable sending auto-discovery short-cut messages.			
Option	Description									
<i>enable</i>	Enable sending auto-discovery short-cut messages.									
<i>disable</i>	Disable sending auto-discovery short-cut messages.									
auto-discovery-shortcuts	Control deletion of child short-cut tunnels when the parent tunnel goes down.	option	-	independent						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>independent</i></td><td>Short-cut tunnels remain up if the parent tunnel goes down.</td></tr><tr><td><i>dependent</i></td><td>Short-cut tunnels are brought down if the parent tunnel goes down.</td></tr></table>	Option	Description	<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.	<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.			
Option	Description									
<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.									
<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.									
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic initiation of IKE SA negotiation.</td></tr><tr><td><i>disable</i></td><td>Disable automatic initiation of IKE SA negotiation.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.			
Option	Description									
<i>enable</i>	Enable automatic initiation of IKE SA negotiation.									
<i>disable</i>	Disable automatic initiation of IKE SA negotiation.									
auto-transport-threshold	Timeout in seconds before falling back to next transport protocol.	integer	Minimum value: 15 1 Maximum value: 300							

Parameter	Description	Type	Size	Default										
azure-ad-autoconnect	Enable/disable Azure AD Auto-Connect for FortiClient.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Azure AD Auto-Connect for FortiClient.</td></tr><tr><td>disable</td><td>Disable Azure AD Auto-Connect for FortiClient.</td></tr></table>	Option	Description	enable	Enable Azure AD Auto-Connect for FortiClient.	disable	Disable Azure AD Auto-Connect for FortiClient.							
Option	Description													
enable	Enable Azure AD Auto-Connect for FortiClient.													
disable	Disable Azure AD Auto-Connect for FortiClient.													
backup-gateway<address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79											
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024											
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr><tr><td>disable</td><td>Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr></table>	Option	Description	enable	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	disable	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.							
Option	Description													
enable	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.													
disable	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.													
cert-peer-username-strip	Enable/disable domain stripping on certificate identity.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable domain stripping on certificate identity.</td></tr><tr><td>enable</td><td>Enable domain stripping on certificate identity.</td></tr></table>	Option	Description	disable	Disable domain stripping on certificate identity.	enable	Enable domain stripping on certificate identity.							
Option	Description													
disable	Disable domain stripping on certificate identity.													
enable	Enable domain stripping on certificate identity.													
cert-peer-username-validation	Enable/disable cross validation of peer username and the identity in the peer's certificate.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Disable cross validation of peer username and the identity in the peer's certificate.</td></tr><tr><td>othername</td><td>Validate principal name in SAN othername.</td></tr><tr><td>rfc822name</td><td>Validate RFC822 email address in SAN.</td></tr><tr><td>cn</td><td>Validate CN in subject.</td></tr></table>	Option	Description	none	Disable cross validation of peer username and the identity in the peer's certificate.	othername	Validate principal name in SAN othername.	rfc822name	Validate RFC822 email address in SAN.	cn	Validate CN in subject.			
Option	Description													
none	Disable cross validation of peer username and the identity in the peer's certificate.													
othername	Validate principal name in SAN othername.													
rfc822name	Validate RFC822 email address in SAN.													
cn	Validate CN in subject.													

Parameter	Description	Type	Size	Default						
cert-trust-store	CA certificate trust store.	option	-	local						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>local</td><td>Use local CA certificate.</td></tr><tr><td>ems</td><td>Use EMS CA certificate.</td></tr></table>	Option	Description	local	Use local CA certificate.	ems	Use EMS CA certificate.			
Option	Description									
local	Use local CA certificate.									
ems	Use EMS CA certificate.									
certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79							
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable childless IKEv2 initiation (RFC 6023).</td></tr><tr><td>disable</td><td>Disable childless IKEv2 initiation (RFC 6023).</td></tr></table>	Option	Description	enable	Enable childless IKEv2 initiation (RFC 6023).	disable	Disable childless IKEv2 initiation (RFC 6023).			
Option	Description									
enable	Enable childless IKEv2 initiation (RFC 6023).									
disable	Disable childless IKEv2 initiation (RFC 6023).									
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable allowing the VPN client to bring up the tunnel when there is no traffic.</td></tr><tr><td>enable</td><td>Enable allowing the VPN client to bring up the tunnel when there is no traffic.</td></tr></table>	Option	Description	disable	Disable allowing the VPN client to bring up the tunnel when there is no traffic.	enable	Enable allowing the VPN client to bring up the tunnel when there is no traffic.			
Option	Description									
disable	Disable allowing the VPN client to bring up the tunnel when there is no traffic.									
enable	Enable allowing the VPN client to bring up the tunnel when there is no traffic.									
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable allowing the VPN client to keep the tunnel up when there is no traffic.</td></tr><tr><td>enable</td><td>Enable allowing the VPN client to keep the tunnel up when there is no traffic.</td></tr></table>	Option	Description	disable	Disable allowing the VPN client to keep the tunnel up when there is no traffic.	enable	Enable allowing the VPN client to keep the tunnel up when there is no traffic.			
Option	Description									
disable	Disable allowing the VPN client to keep the tunnel up when there is no traffic.									
enable	Enable allowing the VPN client to keep the tunnel up when there is no traffic.									

Parameter	Description	Type	Size	Default						
client-resume	Enable/disable resumption of offline FortiClient sessions. When a FortiClient enabled laptop is closed or enters sleep/hibernate mode, enabling this feature allows FortiClient to keep the tunnel during this period, and allows users to immediately resume using the IPsec tunnel when the device wakes up.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable client session resumption.</td></tr><tr><td>disable</td><td>Disable client session resumption.</td></tr></table>	Option	Description	enable	Enable client session resumption.	disable	Disable client session resumption.			
Option	Description									
enable	Enable client session resumption.									
disable	Disable client session resumption.									
client-resume-interval	Maximum time in seconds during which a VPN client may resume using a tunnel after a client PC has entered sleep mode or temporarily lost its network connection (120 - 172800, default = 7200).	integer	Minimum value: 120 Maximum value: 172800	7200						
comments	Comment.	var-string	Maximum length: 255							
default-gw	IPv4 address of default route gateway to use for traffic exiting the interface.	ipv4-address	Not Specified	0.0.0.0						
default-gw-priority	Priority for default gateway route. A higher priority number signifies a less preferred route.	integer	Minimum value: 0 Maximum value: 4294967295	0						
dev-id	Device ID carried by the device ID notification.	string	Maximum length: 63							
dev-id-notification	Enable/disable device ID notification.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable device ID notification.</td></tr><tr><td>enable</td><td>Enable device ID notification.</td></tr></table>	Option	Description	disable	Disable device ID notification.	enable	Enable device ID notification.			
Option	Description									
disable	Disable device ID notification.									
enable	Enable device ID notification.									

Parameter	Description	Type	Size	Default
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified	0.0.0.0
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified	::
dhgrp	DH group.	option	-	14
	Option	Description		
	1	DH Group 1.		
	2	DH Group 2.		
	5	DH Group 5.		
	14	DH Group 14.		
	15	DH Group 15.		
	16	DH Group 16.		
	17	DH Group 17.		
	18	DH Group 18.		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
	27	DH Group 27.		
	28	DH Group 28.		
	29	DH Group 29.		
	30	DH Group 30.		
	31	DH Group 31.		
	32	DH Group 32.		
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable
	Option	Description		
	enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).		
	disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).		

Parameter	Description	Type	Size	Default								
distance	Distance for routes added by IKE (1 - 255).	integer	Minimum value: 1 Maximum value: 255	15								
dns-mode	DNS server mode.	option	-	manual								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>manual</i></td><td>Manually configure DNS servers.</td></tr><tr><td><i>auto</i></td><td>Use default DNS servers.</td></tr></table>	Option	Description	<i>manual</i>	Manually configure DNS servers.	<i>auto</i>	Use default DNS servers.					
Option	Description											
<i>manual</i>	Manually configure DNS servers.											
<i>auto</i>	Use default DNS servers.											
domain	Instruct unity clients about the single default DNS domain.	string	Maximum length: 63									
dpd	Dead Peer Detection mode.	option	-	on-demand								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Dead Peer Detection.</td></tr><tr><td><i>on-idle</i></td><td>Trigger Dead Peer Detection when IPsec is idle.</td></tr><tr><td><i>on-demand</i></td><td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td></tr></table>	Option	Description	<i>disable</i>	Disable Dead Peer Detection.	<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.	<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.			
Option	Description											
<i>disable</i>	Disable Dead Peer Detection.											
<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.											
<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.											
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3								
dpd-retryinterval	DPD retry interval.	user	Not Specified									
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 EAP authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 EAP authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 EAP authentication.	<i>disable</i>	Disable IKEv2 EAP authentication.					
Option	Description											
<i>enable</i>	Enable IKEv2 EAP authentication.											
<i>disable</i>	Disable IKEv2 EAP authentication.											
eap-cert-auth	Enable/disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.</td></tr><tr><td><i>disable</i></td><td>Disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.</td></tr></table>	Option	Description	<i>enable</i>	Enable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.	<i>disable</i>	Disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.					
Option	Description											
<i>enable</i>	Enable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.											
<i>disable</i>	Disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.											

Parameter	Description	Type	Size	Default										
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35											
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-id-payload</i></td><td>Use IKEv2 IDi payload to resolve peer identity.</td></tr><tr><td><i>send-request</i></td><td>Use EAP identity request to resolve peer identity.</td></tr></table>				Option	Description	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.	<i>send-request</i>	Use EAP identity request to resolve peer identity.				
	Option	Description												
	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.												
<i>send-request</i>	Use EAP identity request to resolve peer identity.													
ems-sn-check	Enable/disable verification of EMS serial number.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EMS serial number verification.</td></tr><tr><td><i>disable</i></td><td>Disable EMS serial number verification.</td></tr></table>				Option	Description	<i>enable</i>	Enable EMS serial number verification.	<i>disable</i>	Disable EMS serial number verification.				
	Option	Description												
	<i>enable</i>	Enable EMS serial number verification.												
<i>disable</i>	Disable EMS serial number verification.													
encap-local-gw4	Local IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified	0.0.0.0										
encap-local-gw6	Local IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified	::										
encap-remote-gw4	Remote IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified	0.0.0.0										
encap-remote-gw6	Remote IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified	::										
encapsulation	Enable/disable GRE/VXLAN/VPNID encapsulation.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No additional encapsulation.</td></tr><tr><td><i>gre</i></td><td>GRE encapsulation.</td></tr><tr><td><i>vxlan</i></td><td>VXLAN encapsulation.</td></tr><tr><td><i>vpn-id-ipip</i></td><td>VPN ID with IPIP encapsulation.</td></tr></table>				Option	Description	<i>none</i>	No additional encapsulation.	<i>gre</i>	GRE encapsulation.	<i>vxlan</i>	VXLAN encapsulation.	<i>vpn-id-ipip</i>	VPN ID with IPIP encapsulation.
	Option	Description												
	<i>none</i>	No additional encapsulation.												
	<i>gre</i>	GRE encapsulation.												
	<i>vxlan</i>	VXLAN encapsulation.												
<i>vpn-id-ipip</i>	VPN ID with IPIP encapsulation.													
encapsulation-address	Source for GRE/VXLAN tunnel address.	option	-	ike										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ike</i></td><td>Use IKE/IPsec gateway addresses.</td></tr></table>				Option	Description	<i>ike</i>	Use IKE/IPsec gateway addresses.						
	Option	Description												
<i>ike</i>	Use IKE/IPsec gateway addresses.													

Parameter	Description	Type	Size	Default
	Option	Description		
	ipv4	Specify separate GRE/VXLAN tunnel address.		
	ipv6	Specify separate GRE/VXLAN tunnel address.		
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable
	Option	Description		
	disable	Disable peer ID uniqueness enforcement.		
	keep-new	Enforce peer ID uniqueness, keep new connection if collision found.		
	keep-old	Enforce peer ID uniqueness, keep old connection if collision found.		
esn *	Extended sequence number (ESN) negotiation.	option	-	disable
	Option	Description		
	require	Require extended sequence number.		
	allow	Allow extended sequence number.		
	disable	Disable extended sequence number.		
exchange-fgt-device-id	Enable/disable device identifier exchange with peer FortiGate units for use of VPN monitor data by FortiManager.	option	-	disable
	Option	Description		
	enable	Enable exchange of FortiGate device identifier.		
	disable	Disable exchange of FortiGate device identifier.		
exchange-interface-ip	Enable/disable exchange of IPsec interface IP address.	option	-	disable
	Option	Description		
	enable	Enable exchange of IPsec interface IP address.		
	disable	Disable exchange of IPsec interface IP address.		
exchange-ip-addr4	IPv4 address to exchange with peers.	ipv4-address	Not Specified	0.0.0.0
exchange-ip-addr6	IPv6 address to exchange with peers.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default						
fec-base	Number of base Forward Error Correction packets (1 - 20).	integer	Minimum value: 1 Maximum value: 20	10						
fec-codec	Forward Error Correction encoding/decoding algorithm.	option	-	rs						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>rs</td><td>Reed-Solomon FEC algorithm.</td></tr><tr><td>xor</td><td>XOR FEC algorithm.</td></tr></table>	Option	Description	rs	Reed-Solomon FEC algorithm.	xor	XOR FEC algorithm.			
Option	Description									
rs	Reed-Solomon FEC algorithm.									
xor	XOR FEC algorithm.									
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Forward Error Correction for egress IPsec traffic.</td></tr><tr><td>disable</td><td>Disable Forward Error Correction for egress IPsec traffic.</td></tr></table>	Option	Description	enable	Enable Forward Error Correction for egress IPsec traffic.	disable	Disable Forward Error Correction for egress IPsec traffic.			
Option	Description									
enable	Enable Forward Error Correction for egress IPsec traffic.									
disable	Disable Forward Error Correction for egress IPsec traffic.									
fec-health-check	SD-WAN health check.	string	Maximum length: 35							
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Forward Error Correction for ingress IPsec traffic.</td></tr><tr><td>disable</td><td>Disable Forward Error Correction for ingress IPsec traffic.</td></tr></table>	Option	Description	enable	Enable Forward Error Correction for ingress IPsec traffic.	disable	Disable Forward Error Correction for ingress IPsec traffic.			
Option	Description									
enable	Enable Forward Error Correction for ingress IPsec traffic.									
disable	Disable Forward Error Correction for ingress IPsec traffic.									
fec-mapping-profile	Forward Error Correction (FEC) mapping profile.	string	Maximum length: 35							
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets (1 - 1000).	integer	Minimum value: 1 Maximum value: 1000	50						
fec-redundant	Number of redundant Forward Error Correction packets (1 - 5 for reed-solomon, 1 for xor).	integer	Minimum value: 1 Maximum value: 5	1						
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets (1 - 1000).	integer	Minimum value: 1 Maximum value: 1000	5						
fgsp-sync	Enable/disable IPsec syncing of tunnels for FGSP IPsec.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable IPsec syncing of tunnels to other cluster members.		
	<i>disable</i>	Disable IPsec syncing of tunnels to other cluster members.		
fortinet-esp	Enable/disable Fortinet ESP encapsulation.	option	-	disable
	Option Description			
	<i>enable</i>	Enable Fortinet ESP encapsulation.		
	<i>disable</i>	Disable Fortinet ESP encapsulation.		
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable
	Option Description			
	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.		
	<i>disable</i>	Disable intra-IKE fragmentation support.		
fragmentation-mtu	IKE fragmentation MTU (500 - 16000).	integer	Minimum value: 500 Maximum value: 16000	1200
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-	disable
	Option Description			
	<i>enable</i>	Enable IKEv2 IDi group authentication.		
	<i>disable</i>	Disable IKEv2 IDi group authentication.		
group-authentication-secret	Password for IKEv2 ID group authentication. ASCII string or hexadecimal indicated by a leading 0x.	password-3	Not Specified	
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-	enable
	Option Description			
	<i>enable</i>	Enable HA syncing of ESP sequence numbers.		
	<i>disable</i>	Disable HA syncing of ESP sequence numbers.		
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec tunnel idle timeout.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec tunnel idle timeout.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec tunnel idle timeout.	<i>disable</i>	Disable IPsec tunnel idle timeout.			
	Option	Description								
	<i>enable</i>	Enable IPsec tunnel idle timeout.								
<i>disable</i>	Disable IPsec tunnel idle timeout.									
idle-timeoutinterval	IPsec tunnel idle timeout in minutes (5 - 43200).	integer	Minimum value: 15 5 Maximum value: 43200							
ike-version	IKE protocol version.	option	-	1						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Use IKEv1 protocol.</td></tr><tr><td>2</td><td>Use IKEv2 protocol.</td></tr></table>	Option	Description	1	Use IKEv1 protocol.	2	Use IKEv2 protocol.			
	Option	Description								
	1	Use IKEv1 protocol.								
2	Use IKEv2 protocol.									
inbound-dscp-copy	Enable/disable copy the dscp in the ESP header to the inner IP Header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable copy the dscp in the ESP header to the inner IP Header.</td></tr><tr><td><i>disable</i></td><td>Disable copy the dscp in the ESP header to the inner IP Header.</td></tr></table>	Option	Description	<i>enable</i>	Enable copy the dscp in the ESP header to the inner IP Header.	<i>disable</i>	Disable copy the dscp in the ESP header to the inner IP Header.			
	Option	Description								
	<i>enable</i>	Enable copy the dscp in the ESP header to the inner IP Header.								
<i>disable</i>	Disable copy the dscp in the ESP header to the inner IP Header.									
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable local LAN access on Unity clients.</td></tr><tr><td><i>enable</i></td><td>Enable local LAN access on Unity clients.</td></tr></table>	Option	Description	<i>disable</i>	Disable local LAN access on Unity clients.	<i>enable</i>	Enable local LAN access on Unity clients.			
	Option	Description								
	<i>disable</i>	Disable local LAN access on Unity clients.								
<i>enable</i>	Enable local LAN access on Unity clients.									
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35							
internal-domain-list <domain-name>	One or more internal domain names in quotes separated by spaces. Domain name.	string	Maximum length: 79							
ip-delay-interval	IP address reuse delay interval in seconds (0 - 28800).	integer	Minimum value: 0 0 Maximum value: 28800							
ip-fragmentation	Determine whether IP packets are fragmented before or after IPsec encapsulation.	option	-	post-encapsulation						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pre-encapsulation</i></td><td>Fragment before IPsec encapsulation.</td></tr><tr><td><i>post-encapsulation</i></td><td>Fragment after IPsec encapsulation (RFC compliant).</td></tr></table>	Option	Description	<i>pre-encapsulation</i>	Fragment before IPsec encapsulation.	<i>post-encapsulation</i>	Fragment after IPsec encapsulation (RFC compliant).			
	Option	Description								
	<i>pre-encapsulation</i>	Fragment before IPsec encapsulation.								
<i>post-encapsulation</i>	Fragment after IPsec encapsulation (RFC compliant).									
ip-version	IP version to use for VPN interface.	option	-	4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for gateways.</td></tr><tr><td>6</td><td>Use IPv6 addressing for gateways.</td></tr></table>	Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.			
	Option	Description								
	4	Use IPv4 addressing for gateways.								
6	Use IPv6 addressing for gateways.									
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0						
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0						
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified	0.0.0.0						
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0						
ipv4-name	IPv4 address name.	string	Maximum length: 79							
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified	255.255.255.255						
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79							
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79							
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0						
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0						
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default						
ipv6-auto-linklocal	Enable/disable auto generation of IPv6 link-local address using last 8 bytes of mode-cfg assigned IPv6 address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable mode-cfg auto configuration of IPv6 link-local address.</td></tr><tr><td><i>disable</i></td><td>Disable mode-cfg auto configuration of IPv6 link-local address.</td></tr></table>				Option	Description	<i>enable</i>	Enable mode-cfg auto configuration of IPv6 link-local address.	<i>disable</i>	Disable mode-cfg auto configuration of IPv6 link-local address.
Option	Description									
<i>enable</i>	Enable mode-cfg auto configuration of IPv6 link-local address.									
<i>disable</i>	Disable mode-cfg auto configuration of IPv6 link-local address.									
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::						
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::						
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified	::						
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified	::						
ipv6-name	IPv6 address name.	string	Maximum length: 79							
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128	128						
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79							
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79							
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified	::						
keepalive	NAT-T keep alive interval.	integer	Minimum value: 5 Maximum value: 900	10						
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400						
kms	Key Management Services server.	string	Maximum length: 35							
link-cost	VPN tunnel underlay link cost.	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address	Not Specified	0.0.0.0
local-gw6	IPv6 address of the local gateway's external interface.	ipv6-address	Not Specified	::
localid	Local ID.	string	Maximum length: 63	
localid-type	Local ID type.	option	-	auto
	Option		Description	
	auto	Select ID type automatically.		
	fqdn	Use fully qualified domain name.		
	user-fqdn	Use user fully qualified domain name.		
	keyid	Use key-id string.		
	address	Use local IP address.		
	asn1dn	Use ASN.1 distinguished name.		
loopback-asymroute	Enable/disable asymmetric routing for IKE traffic on loopback interface.	option	-	enable
	Option		Description	
	enable	Allow ingress/egress IKE traffic to be routed over different interfaces.		
	disable	Ingress/egress IKE traffic must be routed over the same interface.		
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-	disable
	Option		Description	
	disable	Disable.		
	subnet	Enable addition of matching subnet selector.		
	host	Enable addition of host to host selector.		
mode	The ID protection mode used to establish a secure channel.	option	-	main

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aggressive</i></td><td>Aggressive mode.</td></tr><tr><td><i>main</i></td><td>Main mode.</td></tr></table>	Option	Description	<i>aggressive</i>	Aggressive mode.	<i>main</i>	Main mode.					
	Option	Description										
	<i>aggressive</i>	Aggressive mode.										
<i>main</i>	Main mode.											
mode-cfg	Enable/disable configuration method.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Configuration Method.</td></tr><tr><td><i>enable</i></td><td>Enable Configuration Method.</td></tr></table>	Option	Description	<i>disable</i>	Disable Configuration Method.	<i>enable</i>	Enable Configuration Method.					
	Option	Description										
	<i>disable</i>	Disable Configuration Method.										
<i>enable</i>	Enable Configuration Method.											
mode-cfg-allow-client-selector	Enable/disable mode-cfg client to use custom phase2 selectors.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Mode-cfg client to use wildcard selectors.</td></tr><tr><td><i>enable</i></td><td>Mode-cfg client to use custom selectors.</td></tr></table>	Option	Description	<i>disable</i>	Mode-cfg client to use wildcard selectors.	<i>enable</i>	Mode-cfg client to use custom selectors.					
	Option	Description										
	<i>disable</i>	Mode-cfg client to use wildcard selectors.										
<i>enable</i>	Mode-cfg client to use custom selectors.											
monitor <name>	IPsec interface as backup for primary interface. IPsec interface as backup for primary interface.	string	Maximum length: 79									
monitor-hold-down-delay	Time to wait in seconds before recovery once primary re-establishes.	integer	Minimum value: 0 Maximum value: 31536000									
monitor-hold-down-time	Time of day at which to fail back to primary after it re-establishes.	user	Not Specified									
monitor-hold-down-type	Recovery time method when primary interface re-establishes.	option	-	immediate								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>immediate</i></td><td>Fail back immediately after primary recovers.</td></tr><tr><td><i>delay</i></td><td>Number of seconds to delay fail back after primary recovers.</td></tr><tr><td><i>time</i></td><td>Specify a time at which to fail back after primary recovers.</td></tr></table>	Option	Description	<i>immediate</i>	Fail back immediately after primary recovers.	<i>delay</i>	Number of seconds to delay fail back after primary recovers.	<i>time</i>	Specify a time at which to fail back after primary recovers.			
	Option	Description										
	<i>immediate</i>	Fail back immediately after primary recovers.										
	<i>delay</i>	Number of seconds to delay fail back after primary recovers.										
<i>time</i>	Specify a time at which to fail back after primary recovers.											
monitor-hold-down-weekday	Day of the week to recover once primary re-establishes.	option	-	sunday								

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>everyday</i></td><td>Every Day.</td></tr><tr><td><i>sunday</i></td><td>Sunday.</td></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr></table>	Option	Description	<i>everyday</i>	Every Day.	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.			
	Option	Description																				
	<i>everyday</i>	Every Day.																				
	<i>sunday</i>	Sunday.																				
	<i>monday</i>	Monday.																				
	<i>tuesday</i>	Tuesday.																				
	<i>wednesday</i>	Wednesday.																				
	<i>thursday</i>	Thursday.																				
	<i>friday</i>	Friday.																				
<i>saturday</i>	Saturday.																					
monitor-min	Minimum number of links to become degraded before activating this interface. Zero (0) means all links must be down before activating this interface.	integer	Minimum value: 0 0 Maximum value: 4294967295																			
name	IPsec remote gateway name.	string	Maximum length: 15																			
nattraversal	Enable/disable NAT traversal.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec NAT traversal.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec NAT traversal.</td></tr><tr><td><i>forced</i></td><td>Force IPsec NAT traversal on.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec NAT traversal.	<i>disable</i>	Disable IPsec NAT traversal.	<i>forced</i>	Force IPsec NAT traversal on.													
	Option	Description																				
	<i>enable</i>	Enable IPsec NAT traversal.																				
	<i>disable</i>	Disable IPsec NAT traversal.																				
<i>forced</i>	Force IPsec NAT traversal on.																					
negotiate-timeout	IKE SA negotiation timeout in seconds (1 - 300).	integer	Minimum value: 30 1 Maximum value: 300																			
net-device	Enable/disable kernel device creation.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Create a kernel device for every tunnel.</td></tr><tr><td><i>disable</i></td><td>Do not create a kernel device for tunnels.</td></tr></table>	Option	Description	<i>enable</i>	Create a kernel device for every tunnel.	<i>disable</i>	Do not create a kernel device for tunnels.															
	Option	Description																				
	<i>enable</i>	Create a kernel device for every tunnel.																				
<i>disable</i>	Do not create a kernel device for tunnels.																					
network-id	VPN gateway network ID.	integer	Minimum value: 0 0 Maximum value: 255																			

Parameter	Description	Type	Size	Default								
network-overlay	Enable/disable network overlays.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable network overlays.</td></tr><tr><td><i>enable</i></td><td>Enable network overlays.</td></tr></table>	Option	Description	<i>disable</i>	Disable network overlays.	<i>enable</i>	Enable network overlays.					
Option	Description											
<i>disable</i>	Disable network overlays.											
<i>enable</i>	Enable network overlays.											
npu-offload *	Enable/disable offloading NPU.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU offloading.</td></tr><tr><td><i>disable</i></td><td>Disable NPU offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU offloading.	<i>disable</i>	Disable NPU offloading.					
Option	Description											
<i>enable</i>	Enable NPU offloading.											
<i>disable</i>	Disable NPU offloading.											
packet-redistribution *	Enable/disable packet distribution (RPS) on the IPsec interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable packet redistribution.</td></tr><tr><td><i>disable</i></td><td>Disable packet redistribution.</td></tr></table>	Option	Description	<i>enable</i>	Enable packet redistribution.	<i>disable</i>	Disable packet redistribution.					
Option	Description											
<i>enable</i>	Enable packet redistribution.											
<i>disable</i>	Disable packet redistribution.											
passive-mode	Enable/disable IPsec passive mode for static tunnels.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec passive mode.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec passive mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec passive mode.	<i>disable</i>	Disable IPsec passive mode.					
Option	Description											
<i>enable</i>	Enable IPsec passive mode.											
<i>disable</i>	Disable IPsec passive mode.											
peer	Accept this peer certificate.	string	Maximum length: 35									
peergrp	Accept this peer certificate group.	string	Maximum length: 35									
peerid	Accept this peer identity.	string	Maximum length: 255									
peertype	Accept this peer type.	option	-	peer								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept any peer ID.</td></tr><tr><td><i>one</i></td><td>Accept this peer ID.</td></tr><tr><td><i>dialup</i></td><td>Accept peer ID in dialup group.</td></tr></table>	Option	Description	<i>any</i>	Accept any peer ID.	<i>one</i>	Accept this peer ID.	<i>dialup</i>	Accept peer ID in dialup group.			
Option	Description											
<i>any</i>	Accept any peer ID.											
<i>one</i>	Accept this peer ID.											
<i>dialup</i>	Accept peer ID in dialup group.											

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>peer</i></td><td>Accept this peer certificate.</td></tr><tr><td><i>peergrp</i></td><td>Accept this peer certificate group.</td></tr></table>	Option	Description	<i>peer</i>	Accept this peer certificate.	<i>peergrp</i>	Accept this peer certificate group.																			
	Option	Description																								
	<i>peer</i>	Accept this peer certificate.																								
<i>peergrp</i>	Accept this peer certificate group.																									
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>allow</i></td><td>Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>require</i></td><td>Require use of IKEv2 Postquantum Preshared Key (PPK).</td></tr></table>	Option	Description	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).																	
	Option	Description																								
	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).																								
	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).																								
<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).																									
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35																							
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																							
priority	Priority for routes added by IKE (1 - 65535).	integer	Minimum value: 1 1 Maximum value: 65535																							
proposal	Phase1 proposal.	option	-																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>des-md5</i></td><td>des-md5</td></tr><tr><td><i>des-sha1</i></td><td>des-sha1</td></tr><tr><td><i>des-sha256</i></td><td>des-sha256</td></tr><tr><td><i>des-sha384</i></td><td>des-sha384</td></tr><tr><td><i>des-sha512</i></td><td>des-sha512</td></tr><tr><td><i>3des-md5</i></td><td>3des-md5</td></tr><tr><td><i>3des-sha1</i></td><td>3des-sha1</td></tr><tr><td><i>3des-sha256</i></td><td>3des-sha256</td></tr><tr><td><i>3des-sha384</i></td><td>3des-sha384</td></tr><tr><td><i>3des-sha512</i></td><td>3des-sha512</td></tr></table>	Option	Description	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1	<i>3des-sha256</i>	3des-sha256	<i>3des-sha384</i>	3des-sha384	<i>3des-sha512</i>	3des-sha512			
	Option	Description																								
	<i>des-md5</i>	des-md5																								
	<i>des-sha1</i>	des-sha1																								
	<i>des-sha256</i>	des-sha256																								
	<i>des-sha384</i>	des-sha384																								
	<i>des-sha512</i>	des-sha512																								
	<i>3des-md5</i>	3des-md5																								
	<i>3des-sha1</i>	3des-sha1																								
	<i>3des-sha256</i>	3des-sha256																								
	<i>3des-sha384</i>	3des-sha384																								
<i>3des-sha512</i>	3des-sha512																									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>aes128-md5</i>	aes128-md5		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1		
	<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256		
	<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384		
	<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1		
	<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256		
	<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384		
	<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512		
	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1		
	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256		
	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384		
	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		

Parameter	Description	Type	Size	Default																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria128-sha256</i></td><td>aria128-sha256</td></tr><tr><td><i>aria128-sha384</i></td><td>aria128-sha384</td></tr><tr><td><i>aria128-sha512</i></td><td>aria128-sha512</td></tr><tr><td><i>aria192-md5</i></td><td>aria192-md5</td></tr><tr><td><i>aria192-sha1</i></td><td>aria192-sha1</td></tr><tr><td><i>aria192-sha256</i></td><td>aria192-sha256</td></tr><tr><td><i>aria192-sha384</i></td><td>aria192-sha384</td></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>aria128-sha256</i>	aria128-sha256	<i>aria128-sha384</i>	aria128-sha384	<i>aria128-sha512</i>	aria128-sha512	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
	Option	Description																																								
	<i>aria128-sha256</i>	aria128-sha256																																								
	<i>aria128-sha384</i>	aria128-sha384																																								
	<i>aria128-sha512</i>	aria128-sha512																																								
	<i>aria192-md5</i>	aria192-md5																																								
	<i>aria192-sha1</i>	aria192-sha1																																								
	<i>aria192-sha256</i>	aria192-sha256																																								
	<i>aria192-sha384</i>	aria192-sha384																																								
	<i>aria192-sha512</i>	aria192-sha512																																								
	<i>aria256-md5</i>	aria256-md5																																								
	<i>aria256-sha1</i>	aria256-sha1																																								
	<i>aria256-sha256</i>	aria256-sha256																																								
	<i>aria256-sha384</i>	aria256-sha384																																								
	<i>aria256-sha512</i>	aria256-sha512																																								
	<i>seed-md5</i>	seed-md5																																								
	<i>seed-sha1</i>	seed-sha1																																								
	<i>seed-sha256</i>	seed-sha256																																								
	<i>seed-sha384</i>	seed-sha384																																								
<i>seed-sha512</i>	seed-sha512																																									
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																																							
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																																							
qkd	Enable/disable use of Quantum Key Distribution (QKD) server.	option	-	disable																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of a Quantum Key Distribution (QKD) server.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of a Quantum Key Distribution (QKD) server.																																					
	Option	Description																																								
<i>disable</i>	Disable use of a Quantum Key Distribution (QKD) server.																																									

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow, but do not require, use of a Quantum Key Distribution (QKD) server.</td></tr><tr><td><i>require</i></td><td>Require use of a Quantum Key Distribution (QKD) server.</td></tr></table>	Option	Description	<i>allow</i>	Allow, but do not require, use of a Quantum Key Distribution (QKD) server.	<i>require</i>	Require use of a Quantum Key Distribution (QKD) server.					
	Option	Description										
	<i>allow</i>	Allow, but do not require, use of a Quantum Key Distribution (QKD) server.										
<i>require</i>	Require use of a Quantum Key Distribution (QKD) server.											
qkd-hybrid	Enable/disable use of Quantum Key Distribution (QKD) hybrid keys.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of Quantum Key Distribution (QKD) hybrid keys.</td></tr><tr><td><i>allow</i></td><td>Allow, but do not require, use of Quantum Key Distribution (QKD) hybrid keys.</td></tr><tr><td><i>require</i></td><td>Require use of Quantum Key Distribution (QKD) hybrid keys.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of Quantum Key Distribution (QKD) hybrid keys.	<i>allow</i>	Allow, but do not require, use of Quantum Key Distribution (QKD) hybrid keys.	<i>require</i>	Require use of Quantum Key Distribution (QKD) hybrid keys.			
	Option	Description										
	<i>disable</i>	Disable use of Quantum Key Distribution (QKD) hybrid keys.										
	<i>allow</i>	Allow, but do not require, use of Quantum Key Distribution (QKD) hybrid keys.										
<i>require</i>	Require use of Quantum Key Distribution (QKD) hybrid keys.											
qkd-profile	Quantum Key Distribution (QKD) server profile.	string	Maximum length: 35									
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IKE SA re-authentication.</td></tr><tr><td><i>enable</i></td><td>Enable IKE SA re-authentication.</td></tr></table>	Option	Description	<i>disable</i>	Disable IKE SA re-authentication.	<i>enable</i>	Enable IKE SA re-authentication.					
	Option	Description										
	<i>disable</i>	Disable IKE SA re-authentication.										
<i>enable</i>	Enable IKE SA re-authentication.											
rekey	Enable/disable phase1 rekey.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable phase1 rekey.</td></tr><tr><td><i>disable</i></td><td>Disable phase1 rekey.</td></tr></table>	Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.					
	Option	Description										
	<i>enable</i>	Enable phase1 rekey.										
<i>disable</i>	Disable phase1 rekey.											
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0								
remote-gw-country	IPv4 addresses associated to a specific country.	string	Maximum length: 2									
remote-gw-end-ip	Last IPv4 address in the range.	ipv4-address-any	Not Specified	0.0.0.0								
remote-gw-match	Set type of IPv4 remote gateway address matching.	option	-	any								

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Match any IPv4 gateway address.</td></tr><tr><td><i>ipmask</i></td><td>Match IPv4 gateway address and mask.</td></tr><tr><td><i>iprange</i></td><td>Match IPv4 gateway address range.</td></tr><tr><td><i>geography</i></td><td>Match IPv4 gateway address from a specified country.</td></tr><tr><td><i>ztna</i></td><td>Match IPv4 gateway address against ZTNA posture tags.</td></tr></table>	Option	Description	<i>any</i>	Match any IPv4 gateway address.	<i>ipmask</i>	Match IPv4 gateway address and mask.	<i>iprange</i>	Match IPv4 gateway address range.	<i>geography</i>	Match IPv4 gateway address from a specified country.	<i>ztna</i>	Match IPv4 gateway address against ZTNA posture tags.			
	Option	Description														
	<i>any</i>	Match any IPv4 gateway address.														
	<i>ipmask</i>	Match IPv4 gateway address and mask.														
	<i>iprange</i>	Match IPv4 gateway address range.														
	<i>geography</i>	Match IPv4 gateway address from a specified country.														
<i>ztna</i>	Match IPv4 gateway address against ZTNA posture tags.															
remote-gw-start-ip	First IPv4 address in the range.	ipv4-address-any	Not Specified	0.0.0.0												
remote-gw-subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0												
remote-gw-ztna-tags <name>	IPv4 ZTNA posture tags. Address name.	string	Maximum length: 79													
remote-gw6	IPv6 address of the remote gateway's external interface.	ipv6-address	Not Specified	::												
remote-gw6-country	IPv6 addresses associated to a specific country.	string	Maximum length: 2													
remote-gw6-end-ip	Last IPv6 address in the range.	ipv6-address	Not Specified	::												
remote-gw6-match	Set type of IPv6 remote gateway address matching.	option	-	any												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Match any IPv6 gateway address.</td></tr><tr><td><i>ipprefix</i></td><td>Match IPv6 gateway address and prefix.</td></tr><tr><td><i>iprange</i></td><td>Match IPv6 gateway address range.</td></tr><tr><td><i>geography</i></td><td>Match IPv6 gateway address from a specified country.</td></tr></table>	Option	Description	<i>any</i>	Match any IPv6 gateway address.	<i>ipprefix</i>	Match IPv6 gateway address and prefix.	<i>iprange</i>	Match IPv6 gateway address range.	<i>geography</i>	Match IPv6 gateway address from a specified country.					
	Option	Description														
	<i>any</i>	Match any IPv6 gateway address.														
	<i>ipprefix</i>	Match IPv6 gateway address and prefix.														
	<i>iprange</i>	Match IPv6 gateway address range.														
<i>geography</i>	Match IPv6 gateway address from a specified country.															
remote-gw6-start-ip	First IPv6 address in the range.	ipv6-address	Not Specified	::												
remote-gw6-subnet	IPv6 address and prefix.	ipv6-network	Not Specified	::/0												
remotegw-ddns	Domain name of remote gateway. For example, name.ddns.com.	string	Maximum length: 63													
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-	pkcs1												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.		
	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).		
rsa-signature-hash-override	Enable/disable IKEv2 RSA signature hash algorithm override.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IKEv2 RSA signature hash algorithm override.		
	<i>disable</i>	Disable IKEv2 RSA signature hash algorithm override.		
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable saving XAuth username and password on VPN clients.		
	<i>enable</i>	Enable saving XAuth username and password on VPN clients.		
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sending certificate chain.		
	<i>disable</i>	Disable sending certificate chain.		
shared-idle-timeout	Enable/disable IPsec tunnel shared idle timeout.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPsec tunnel shared idle timeout. The location-id attribute must be configured on both spokes. Shared idle timeout is supported only on IKEv2 since remote-location is available only for IKEv2.		
	<i>disable</i>	Disable IPsec tunnel shared idle timeout.		
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha1</td><td>SHA1.</td></tr><tr><td>sha2-256</td><td>SHA2-256.</td></tr><tr><td>sha2-384</td><td>SHA2-384.</td></tr><tr><td>sha2-512</td><td>SHA2-512.</td></tr></table>	Option	Description	sha1	SHA1.	sha2-256	SHA2-256.	sha2-384	SHA2-384.	sha2-512	SHA2-512.			
	Option	Description												
	sha1	SHA1.												
	sha2-256	SHA2-256.												
	sha2-384	SHA2-384.												
sha2-512	SHA2-512.													
split-include-service	Split-include services.	string	Maximum length: 79											
suite-b	Use Suite-B.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not use UI suite.</td></tr><tr><td>suite-b-gcm-128</td><td>Use Suite-B-GCM-128.</td></tr><tr><td>suite-b-gcm-256</td><td>Use Suite-B-GCM-256.</td></tr></table>	Option	Description	disable	Do not use UI suite.	suite-b-gcm-128	Use Suite-B-GCM-128.	suite-b-gcm-256	Use Suite-B-GCM-256.					
	Option	Description												
	disable	Do not use UI suite.												
	suite-b-gcm-128	Use Suite-B-GCM-128.												
	suite-b-gcm-256	Use Suite-B-GCM-256.												
transport	Set IKE transport protocol.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Use UDP transport for IKE.</td></tr><tr><td>auto</td><td>Use AUTO transport for IKE.</td></tr><tr><td>tcp</td><td>Use TCP transport for IKE.</td></tr></table>	Option	Description	udp	Use UDP transport for IKE.	auto	Use AUTO transport for IKE.	tcp	Use TCP transport for IKE.					
	Option	Description												
	udp	Use UDP transport for IKE.												
	auto	Use AUTO transport for IKE.												
	tcp	Use TCP transport for IKE.												
type	Remote gateway type.	option	-	static										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Remote VPN gateway has fixed IP address.</td></tr><tr><td>dynamic</td><td>Remote VPN gateway has dynamic IP address.</td></tr><tr><td>ddns</td><td>Remote VPN gateway has dynamic IP address and is a dynamic DNS client.</td></tr></table>	Option	Description	static	Remote VPN gateway has fixed IP address.	dynamic	Remote VPN gateway has dynamic IP address.	ddns	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.					
	Option	Description												
	static	Remote VPN gateway has fixed IP address.												
	dynamic	Remote VPN gateway has dynamic IP address.												
	ddns	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.												
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Cisco Unity Configuration Method Extensions.</td></tr><tr><td>enable</td><td>Enable Cisco Unity Configuration Method Extensions.</td></tr></table>	Option	Description	disable	Disable Cisco Unity Configuration Method Extensions.	enable	Enable Cisco Unity Configuration Method Extensions.							
	Option	Description												
	disable	Disable Cisco Unity Configuration Method Extensions.												
enable	Enable Cisco Unity Configuration Method Extensions.													

Parameter	Description	Type	Size	Default
usrgrp	User group name for dialup peers.	string	Maximum length: 35	
vni	VNI of VXLAN tunnel.	integer	Minimum value: 0 1 Maximum value: 16777215	
wizard-type	GUI VPN Wizard Type.	option	-	custom
	Option	Description		
	custom	Custom VPN configuration.		
	dialup-forticlient	Dial Up - FortiClient Windows, Mac and Android.		
	dialup-ios	Dial Up - iPhone / iPad Native IPsec Client.		
	dialup-android	Dial Up - Android Native IPsec Client.		
	dialup-windows	Dial Up - Windows Native IPsec Client.		
	dialup-cisco	Dial Up - Cisco IPsec Client.		
	static-fortigate	Site to Site - FortiGate.		
	dialup-fortigate	Dial Up - FortiGate.		
	static-cisco	Site to Site - Cisco.		
	dialup-cisco-fw	Dialup Up - Cisco Firewall.		
	simplified-static-fortigate	Site to Site - FortiGate (SD-WAN).		
	hub-fortigate-auto-discovery	Hub role in a Hub-and-Spoke auto-discovery VPN.		
	spoke-fortigate-auto-discovery	Spoke role in a Hub-and-Spoke auto-discovery VPN.		
	fabric-overlay-orchestrator	Fabric Overlay Orchestrator.		
xauthtype	XAuth type.	option	-	disable
	Option	Description		
	disable	Disable.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>client</i>	Enable as client.		
	<i>pap</i>	Enable as server PAP.		
	<i>chap</i>	Enable as server CHAP.		
	<i>auto</i>	Enable as server auto.		

* This parameter may not exist in some models.

config ipv4-exclude-range

Parameter	Description	Type	Size	Default
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0

config ipv6-exclude-range

Parameter	Description	Type	Size	Default
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified	::
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified	::

config vpn ipsec phase2

Configure VPN autokey tunnel.

```
config vpn ipsec phase2
  Description: Configure VPN autokey tunnel.
```



```

edit <name>
    set add-route [phase1|enable|...]
    set addke1 {option1}, {option2}, ...
    set addke2 {option1}, {option2}, ...
    set addke3 {option1}, {option2}, ...
    set addke4 {option1}, {option2}, ...
    set addke5 {option1}, {option2}, ...
    set addke6 {option1}, {option2}, ...
    set addke7 {option1}, {option2}, ...
    set auto-negotiate [enable|disable]
    set comments {var-string}
    set dhcp-ipsec [enable|disable]
    set dhgrp {option1}, {option2}, ...
    set diffserv [enable|disable]
    set diffservcode {user}
    set dst-addr-type [subnet|range|...]
    set dst-end-ip {ipv4-address-any}
    set dst-end-ip6 {ipv6-address}
    set dst-name {string}
    set dst-name6 {string}
    set dst-port {integer}
    set dst-start-ip {ipv4-address-any}
    set dst-start-ip6 {ipv6-address}
    set dst-subnet {ipv4-classnet-any}
    set dst-subnet6 {ipv6-prefix}
    set encapsulation [tunnel-mode|transport-mode]
    set inbound-dscp-copy [phase1|enable|...]
    set initiator-ts-narrow [enable|disable]
    set keepalive [enable|disable]
    set keylife-type [seconds|kbs|...]
    set keylifekbs {integer}
    set keylifeseconds {integer}
    set l2tp [enable|disable]
    set pfs [enable|disable]
    set phase1name {string}
    set proposal {option1}, {option2}, ...
    set protocol {integer}
    set replay [enable|disable]
    set route-overlap [use-old|use-new|...]
    set selector-match [exact|subset|...]
    set single-source [enable|disable]
    set src-addr-type [subnet|range|...]
    set src-end-ip {ipv4-address-any}
    set src-end-ip6 {ipv6-address}
    set src-name {string}
    set src-name6 {string}
    set src-port {integer}
    set src-start-ip {ipv4-address-any}
    set src-start-ip6 {ipv6-address}
    set src-subnet {ipv4-classnet-any}
    set src-subnet6 {ipv6-prefix}
    set use-natip [enable|disable]

```

```
next
end
```

config vpn ipsec phase2

Parameter	Description	Type	Size	Default
add-route	Enable/disable automatic route addition.	option	-	phase1
	Option	Description		
	<i>phase1</i>	Add route according to phase1 add-route setting.		
	<i>enable</i>	Add route for remote proxy ID.		
	<i>disable</i>	Do not add route for remote proxy ID.		
addke1	phase2 ADDKE1 group.	option	-	
	Option	Description		
	<i>0</i>	NONE.		
	<i>35</i>	ML-KEM-512.		
	<i>36</i>	ML-KEM-768.		
	<i>37</i>	ML-KEM-1024.		
	<i>1080</i>	KYBER512.		
	<i>1081</i>	KYBER768.		
	<i>1082</i>	KYBER1024.		
	<i>1083</i>	FRODO L1.		
	<i>1084</i>	FRODO L3.		
	<i>1085</i>	FRODO L5.		
	<i>1089</i>	BIKE L1.		
	<i>1090</i>	BIKE L3.		
	<i>1091</i>	BIKE L5.		
	<i>1092</i>	HQC128.		
	<i>1093</i>	HQC192.		
	<i>1094</i>	HQC256.		
addke2	phase2 ADDKE2 group.	option	-	

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					
addke3	phase2 ADDKE3 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.															
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
1085	FRODO L5.																																					

Parameter	Description	Type	Size	Default
	Option	Description		
	1089	BIKE L1.		
	1090	BIKE L3.		
	1091	BIKE L5.		
	1092	HQC128.		
	1093	HQC192.		
	1094	HQC256.		
addke4	phase2 ADDKE4 group.	option	-	
	Option	Description		
	0	NONE.		
	35	ML-KEM-512.		
	36	ML-KEM-768.		
	37	ML-KEM-1024.		
	1080	KYBER512.		
	1081	KYBER768.		
	1082	KYBER1024.		
	1083	FRODO L1.		
	1084	FRODO L3.		
	1085	FRODO L5.		
	1089	BIKE L1.		
	1090	BIKE L3.		
	1091	BIKE L5.		
	1092	HQC128.		
	1093	HQC192.		
	1094	HQC256.		
addke5	phase2 ADDKE5 group.	option	-	
	Option	Description		
	0	NONE.		
	35	ML-KEM-512.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																
	36	ML-KEM-768.																																
	37	ML-KEM-1024.																																
	1080	KYBER512.																																
	1081	KYBER768.																																
	1082	KYBER1024.																																
	1083	FRODO L1.																																
	1084	FRODO L3.																																
	1085	FRODO L5.																																
	1089	BIKE L1.																																
	1090	BIKE L3.																																
	1091	BIKE L5.																																
	1092	HQC128.																																
	1093	HQC192.																																
1094	HQC256.																																	
addke6	phase2 ADDKE6 group.	option	-																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.							
	Option	Description																																
	0	NONE.																																
	35	ML-KEM-512.																																
	36	ML-KEM-768.																																
	37	ML-KEM-1024.																																
	1080	KYBER512.																																
	1081	KYBER768.																																
	1082	KYBER1024.																																
	1083	FRODO L1.																																
	1084	FRODO L3.																																
	1085	FRODO L5.																																
	1089	BIKE L1.																																
	1090	BIKE L3.																																

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.																											
	Option	Description																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					
addke7	phase2 ADDKE7 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
	1094	HQC256.																																				
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.																															
	Option	Description																																				
	enable	Enable setting.																																				
disable	Disable setting.																																					
comments	Comment.	var-string	Maximum length: 255																																			

Parameter	Description	Type	Size	Default
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-	disable
	Option Description			
	enable	Enable setting.		
	disable	Disable setting.		
dhgrp	Phase2 DH group.	option	-	14
	Option Description			
	1	DH Group 1.		
	2	DH Group 2.		
	5	DH Group 5.		
	14	DH Group 14.		
	15	DH Group 15.		
	16	DH Group 16.		
	17	DH Group 17.		
	18	DH Group 18.		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
	27	DH Group 27.		
	28	DH Group 28.		
	29	DH Group 29.		
	30	DH Group 30.		
	31	DH Group 31.		
	32	DH Group 32.		
diffserv	Enable/disable applying DSCP value to the IPsec tunnel outer IP header.	option	-	disable
	Option Description			
	enable	Enable setting.		
	disable	Disable setting.		
diffservcode	DSCP value to be applied to the IPsec tunnel outer IP header.	user	Not Specified	

Parameter	Description	Type	Size	Default										
dst-addr-type	Remote proxy ID type.	option	-	subnet										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>subnet</td><td>IPv4 subnet.</td></tr><tr><td>range</td><td>IPv4 range.</td></tr><tr><td>ip</td><td>IPv4 IP.</td></tr><tr><td>name</td><td>IPv4 firewall address or group name.</td></tr></table>				Option	Description	subnet	IPv4 subnet.	range	IPv4 range.	ip	IPv4 IP.	name	IPv4 firewall address or group name.
	Option	Description												
	subnet	IPv4 subnet.												
	range	IPv4 range.												
	ip	IPv4 IP.												
name	IPv4 firewall address or group name.													
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0										
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified	::										
dst-name	Remote proxy ID name.	string	Maximum length: 79											
dst-name6	Remote proxy ID name.	string	Maximum length: 79											
dst-port	Quick mode destination port (1 - 65535 or 0 for all).	integer	Minimum value: 0 Maximum value: 65535	0										
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0										
dst-start-ip6	Remote proxy ID IPv6 start.	ipv6-address	Not Specified	::										
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0										
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0										
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tunnel-mode</td><td>Use tunnel mode encapsulation.</td></tr><tr><td>transport-mode</td><td>Use transport mode encapsulation.</td></tr></table>				Option	Description	tunnel-mode	Use tunnel mode encapsulation.	transport-mode	Use transport mode encapsulation.				
	Option	Description												
	tunnel-mode	Use tunnel mode encapsulation.												
transport-mode	Use transport mode encapsulation.													
inbound-dscp-copy	Enable/disable copying of the DSCP in the ESP header to the inner IP header.	option	-	phase1										

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.</td></tr><tr><td><i>enable</i></td><td>Enable copying of the DSCP in the ESP header to the inner IP header.</td></tr><tr><td><i>disable</i></td><td>Disable copying of the DSCP in the ESP header to the inner IP header.</td></tr></table>	Option	Description	<i>phase1</i>	copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.	<i>enable</i>	Enable copying of the DSCP in the ESP header to the inner IP header.	<i>disable</i>	Disable copying of the DSCP in the ESP header to the inner IP header.			
	Option	Description										
	<i>phase1</i>	copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.										
	<i>enable</i>	Enable copying of the DSCP in the ESP header to the inner IP header.										
<i>disable</i>	Disable copying of the DSCP in the ESP header to the inner IP header.											
initiator-ts-narrow	Enable/disable traffic selector narrowing for IKEv2 initiator.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
keepalive	Enable/disable keep alive.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
keylife-type	Keylife type.	option	-	seconds								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>seconds</i></td><td>Key life in seconds.</td></tr><tr><td><i>kbs</i></td><td>Key life in kilobytes.</td></tr><tr><td><i>both</i></td><td>Key life both.</td></tr></table>	Option	Description	<i>seconds</i>	Key life in seconds.	<i>kbs</i>	Key life in kilobytes.	<i>both</i>	Key life both.			
	Option	Description										
	<i>seconds</i>	Key life in seconds.										
	<i>kbs</i>	Key life in kilobytes.										
<i>both</i>	Key life both.											
keylifekbs	Phase2 key life in number of kilobytes of traffic (5120 - 4294967295).	integer	Minimum value: 5120 Maximum value: 4294967295									
keylifeseconds	Phase2 key life in time in seconds (120 - 172800).	integer	Minimum value: 120 Maximum value: 172800	43200								
l2tp	Enable/disable L2TP over IPsec.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable L2TP over IPsec.</td></tr><tr><td><i>disable</i></td><td>Disable L2TP over IPsec.</td></tr></table>	Option	Description	<i>enable</i>	Enable L2TP over IPsec.	<i>disable</i>	Disable L2TP over IPsec.					
	Option	Description										
	<i>enable</i>	Enable L2TP over IPsec.										
<i>disable</i>	Disable L2TP over IPsec.											

Parameter	Description	Type	Size	Default																																										
name	IPsec tunnel name.	string	Maximum length: 35																																											
pfs	Enable/disable PFS feature.	option	-	enable																																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																				
	Option	Description																																												
	<i>enable</i>	Enable setting.																																												
<i>disable</i>	Disable setting.																																													
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 35																																											
proposal	Phase2 proposal.	option	-																																											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null-md5</i></td><td>null-md5</td></tr><tr><td><i>null-sha1</i></td><td>null-sha1</td></tr><tr><td><i>null-sha256</i></td><td>null-sha256</td></tr><tr><td><i>null-sha384</i></td><td>null-sha384</td></tr><tr><td><i>null-sha512</i></td><td>null-sha512</td></tr><tr><td><i>des-null</i></td><td>des-null</td></tr><tr><td><i>des-md5</i></td><td>des-md5</td></tr><tr><td><i>des-sha1</i></td><td>des-sha1</td></tr><tr><td><i>des-sha256</i></td><td>des-sha256</td></tr><tr><td><i>des-sha384</i></td><td>des-sha384</td></tr><tr><td><i>des-sha512</i></td><td>des-sha512</td></tr><tr><td><i>3des-null</i></td><td>3des-null</td></tr><tr><td><i>3des-md5</i></td><td>3des-md5</td></tr><tr><td><i>3des-sha1</i></td><td>3des-sha1</td></tr><tr><td><i>3des-sha256</i></td><td>3des-sha256</td></tr><tr><td><i>3des-sha384</i></td><td>3des-sha384</td></tr><tr><td><i>3des-sha512</i></td><td>3des-sha512</td></tr><tr><td><i>aes128-null</i></td><td>aes128-null</td></tr><tr><td><i>aes128-md5</i></td><td>aes128-md5</td></tr><tr><td><i>aes128-sha1</i></td><td>aes128-sha1</td></tr></table>				Option	Description	<i>null-md5</i>	null-md5	<i>null-sha1</i>	null-sha1	<i>null-sha256</i>	null-sha256	<i>null-sha384</i>	null-sha384	<i>null-sha512</i>	null-sha512	<i>des-null</i>	des-null	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-null</i>	3des-null	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1	<i>3des-sha256</i>	3des-sha256	<i>3des-sha384</i>	3des-sha384	<i>3des-sha512</i>	3des-sha512	<i>aes128-null</i>	aes128-null	<i>aes128-md5</i>	aes128-md5	<i>aes128-sha1</i>	aes128-sha1
	Option	Description																																												
	<i>null-md5</i>	null-md5																																												
	<i>null-sha1</i>	null-sha1																																												
	<i>null-sha256</i>	null-sha256																																												
	<i>null-sha384</i>	null-sha384																																												
	<i>null-sha512</i>	null-sha512																																												
	<i>des-null</i>	des-null																																												
	<i>des-md5</i>	des-md5																																												
	<i>des-sha1</i>	des-sha1																																												
	<i>des-sha256</i>	des-sha256																																												
	<i>des-sha384</i>	des-sha384																																												
	<i>des-sha512</i>	des-sha512																																												
	<i>3des-null</i>	3des-null																																												
	<i>3des-md5</i>	3des-md5																																												
	<i>3des-sha1</i>	3des-sha1																																												
	<i>3des-sha256</i>	3des-sha256																																												
	<i>3des-sha384</i>	3des-sha384																																												
	<i>3des-sha512</i>	3des-sha512																																												
	<i>aes128-null</i>	aes128-null																																												
<i>aes128-md5</i>	aes128-md5																																													
<i>aes128-sha1</i>	aes128-sha1																																													

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm</i>	aes128gcm		
	<i>aes192-null</i>	aes192-null		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-null</i>	aes256-null		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm</i>	aes256gcm		
	<i>chacha20poly1305</i>	chacha20poly1305		
	<i>aria128-null</i>	aria128-null		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		
	<i>aria128-sha512</i>	aria128-sha512		
	<i>aria192-null</i>	aria192-null		
	<i>aria192-md5</i>	aria192-md5		
	<i>aria192-sha1</i>	aria192-sha1		
	<i>aria192-sha256</i>	aria192-sha256		
	<i>aria192-sha384</i>	aria192-sha384		

Parameter	Description	Type	Size	Default																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-null</i></td><td>aria256-null</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-null</i></td><td>seed-null</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-null</i>	aria256-null	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-null</i>	seed-null	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512				
	Option	Description																															
	<i>aria192-sha512</i>	aria192-sha512																															
	<i>aria256-null</i>	aria256-null																															
	<i>aria256-md5</i>	aria256-md5																															
	<i>aria256-sha1</i>	aria256-sha1																															
	<i>aria256-sha256</i>	aria256-sha256																															
	<i>aria256-sha384</i>	aria256-sha384																															
	<i>aria256-sha512</i>	aria256-sha512																															
	<i>seed-null</i>	seed-null																															
	<i>seed-md5</i>	seed-md5																															
	<i>seed-sha1</i>	seed-sha1																															
	<i>seed-sha256</i>	seed-sha256																															
	<i>seed-sha384</i>	seed-sha384																															
<i>seed-sha512</i>	seed-sha512																																
protocol	Quick mode protocol selector (1 - 255 or 0 for all).	integer	Minimum value: 0 0 Maximum value: 255	0																													
replay	Enable/disable replay detection.	option	-	enable																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																										
	Option	Description																															
	<i>enable</i>	Enable setting.																															
<i>disable</i>	Disable setting.																																
route-overlap	Action for overlapping routes.	option	-	use-new																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-old</i></td><td>Use the old route and do not add the new route.</td></tr><tr><td><i>use-new</i></td><td>Delete the old route and add the new route.</td></tr><tr><td><i>allow</i></td><td>Allow overlapping routes.</td></tr></table>	Option	Description	<i>use-old</i>	Use the old route and do not add the new route.	<i>use-new</i>	Delete the old route and add the new route.	<i>allow</i>	Allow overlapping routes.																								
	Option	Description																															
	<i>use-old</i>	Use the old route and do not add the new route.																															
	<i>use-new</i>	Delete the old route and add the new route.																															
<i>allow</i>	Allow overlapping routes.																																
selector-match	Match type to use when comparing selectors.	option	-	auto																													

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>exact</i>	Match selectors exactly.		
	<i>subset</i>	Match selectors by subset.		
	<i>auto</i>	Use subset or exact match depending on selector address type.		
single-source	Enable/disable single source IP restriction.	option	-	disable
	Option	Description		
	<i>enable</i>	Only single source IP will be accepted.		
	<i>disable</i>	Source IP range will be accepted.		
src-addr-type	Local proxy ID type.	option	-	subnet
	Option	Description		
	<i>subnet</i>	IPv4 subnet.		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified	::
src-name	Local proxy ID name.	string	Maximum length: 79	
src-name6	Local proxy ID name.	string	Maximum length: 79	
src-port	Quick mode source port (1 - 65535 or 0 for all).	integer	Minimum value: 0 0 Maximum value: 65535	0
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
use-natip	Enable to use the FortiGate public IP as the source selector when outbound NAT is used.	option	-	enable

Option	Description
<i>enable</i>	Replace source selector with interface IP when using outbound NAT.
<i>disable</i>	Do not modify source selector when using outbound NAT.

config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

```

config vpn ipsec phase2-interface
    Description: Configure VPN autokey tunnel.
    edit <name>
        set add-route [phase1|enable|...]
        set addke1 {option1}, {option2}, ...
        set addke2 {option1}, {option2}, ...
        set addke3 {option1}, {option2}, ...
        set addke4 {option1}, {option2}, ...
        set addke5 {option1}, {option2}, ...
        set addke6 {option1}, {option2}, ...
        set addke7 {option1}, {option2}, ...
        set auto-discovery-forwarder [phase1|enable|...]
        set auto-discovery-sender [phase1|enable|...]
        set auto-negotiate [enable|disable]
        set comments {var-string}
        set dhcp-ipsec [enable|disable]
        set dhgrp {option1}, {option2}, ...
        set diffserv [enable|disable]
        set diffservcode {user}
        set dst-addr-type [subnet|range|...]
        set dst-end-ip {ipv4-address-any}
        set dst-end-ip6 {ipv6-address}
        set dst-name {string}
        set dst-name6 {string}
        set dst-port {integer}
        set dst-start-ip {ipv4-address-any}
        set dst-start-ip6 {ipv6-address}
        set dst-subnet {ipv4-classnet-any}
        set dst-subnet6 {ipv6-prefix}
    
```

```

set encapsulation [tunnel-mode|transport-mode]
set inbound-dscp-copy [phase1|enable|...]
set initiator-ts-narrow [enable|disable]
set keepalive [enable|disable]
set keylife-type [seconds|kbs|...]
set keylifekbs {integer}
set keylifeseconds {integer}
set l2tp [enable|disable]
set pfs [enable|disable]
set phase1name {string}
set proposal {option1}, {option2}, ...
set protocol {integer}
set replay [enable|disable]
set route-overlap [use-old|use-new|...]
set single-source [enable|disable]
set src-addr-type [subnet|range|...]
set src-end-ip {ipv4-address-any}
set src-end-ip6 {ipv6-address}
set src-name {string}
set src-name6 {string}
set src-port {integer}
set src-start-ip {ipv4-address-any}
set src-start-ip6 {ipv6-address}
set src-subnet {ipv4-classnet-any}
set src-subnet6 {ipv6-prefix}

next
end

```

config vpn ipsec phase2-interface

Parameter	Description	Type	Size	Default
add-route	Enable/disable automatic route addition.	option	-	phase1
	Option	Description		
	<i>phase1</i>	Add route according to phase1 add-route setting.		
	<i>enable</i>	Add route for remote proxy ID.		
	<i>disable</i>	Do not add route for remote proxy ID.		
addke1	phase2 ADDKE1 group.	option	-	
	Option	Description		
	0	NONE.		
	35	ML-KEM-512.		
	36	ML-KEM-768.		

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																														
	37	ML-KEM-1024.																														
	1080	KYBER512.																														
	1081	KYBER768.																														
	1082	KYBER1024.																														
	1083	FRODO L1.																														
	1084	FRODO L3.																														
	1085	FRODO L5.																														
	1089	BIKE L1.																														
	1090	BIKE L3.																														
	1091	BIKE L5.																														
	1092	HQC128.																														
	1093	HQC192.																														
	1094	HQC256.																														
addke2	phase2 ADDKE2 group.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.			
	Option	Description																														
	0	NONE.																														
	35	ML-KEM-512.																														
	36	ML-KEM-768.																														
	37	ML-KEM-1024.																														
	1080	KYBER512.																														
	1081	KYBER768.																														
	1082	KYBER1024.																														
	1083	FRODO L1.																														
	1084	FRODO L3.																														
	1085	FRODO L5.																														
	1089	BIKE L1.																														
	1090	BIKE L3.																														
	1091	BIKE L5.																														

Parameter	Description	Type	Size	Default
	Option Description			
	1092	HQC128.		
	1093	HQC192.		
	1094	HQC256.		
addke3	phase2 ADDKE3 group.	option	-	
	Option Description			
	0	NONE.		
	35	ML-KEM-512.		
	36	ML-KEM-768.		
	37	ML-KEM-1024.		
	1080	KYBER512.		
	1081	KYBER768.		
	1082	KYBER1024.		
	1083	FRODO L1.		
	1084	FRODO L3.		
	1085	FRODO L5.		
	1089	BIKE L1.		
	1090	BIKE L3.		
	1091	BIKE L5.		
	1092	HQC128.		
	1093	HQC192.		
	1094	HQC256.		
addke4	phase2 ADDKE4 group.	option	-	
	Option Description			
	0	NONE.		
	35	ML-KEM-512.		
	36	ML-KEM-768.		
	37	ML-KEM-1024.		
	1080	KYBER512.		

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.													
	Option	Description																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					
addke5	phase2 ADDKE5 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					

Parameter	Description	Type	Size	Default																																		
addke6	phase2 ADDKE6 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
	1084	FRODO L3.																																				
	1085	FRODO L5.																																				
	1089	BIKE L1.																																				
	1090	BIKE L3.																																				
	1091	BIKE L5.																																				
	1092	HQC128.																																				
	1093	HQC192.																																				
1094	HQC256.																																					
addke7	phase2 ADDKE7 group.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>NONE.</td></tr><tr><td>35</td><td>ML-KEM-512.</td></tr><tr><td>36</td><td>ML-KEM-768.</td></tr><tr><td>37</td><td>ML-KEM-1024.</td></tr><tr><td>1080</td><td>KYBER512.</td></tr><tr><td>1081</td><td>KYBER768.</td></tr><tr><td>1082</td><td>KYBER1024.</td></tr><tr><td>1083</td><td>FRODO L1.</td></tr><tr><td>1084</td><td>FRODO L3.</td></tr></table>	Option	Description	0	NONE.	35	ML-KEM-512.	36	ML-KEM-768.	37	ML-KEM-1024.	1080	KYBER512.	1081	KYBER768.	1082	KYBER1024.	1083	FRODO L1.	1084	FRODO L3.																	
	Option	Description																																				
	0	NONE.																																				
	35	ML-KEM-512.																																				
	36	ML-KEM-768.																																				
	37	ML-KEM-1024.																																				
	1080	KYBER512.																																				
	1081	KYBER768.																																				
	1082	KYBER1024.																																				
	1083	FRODO L1.																																				
1084	FRODO L3.																																					

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1085</td><td>FRODO L5.</td></tr><tr><td>1089</td><td>BIKE L1.</td></tr><tr><td>1090</td><td>BIKE L3.</td></tr><tr><td>1091</td><td>BIKE L5.</td></tr><tr><td>1092</td><td>HQC128.</td></tr><tr><td>1093</td><td>HQC192.</td></tr><tr><td>1094</td><td>HQC256.</td></tr></table>	Option	Description	1085	FRODO L5.	1089	BIKE L1.	1090	BIKE L3.	1091	BIKE L5.	1092	HQC128.	1093	HQC192.	1094	HQC256.			
	Option	Description																		
	1085	FRODO L5.																		
	1089	BIKE L1.																		
	1090	BIKE L3.																		
	1091	BIKE L5.																		
	1092	HQC128.																		
	1093	HQC192.																		
1094	HQC256.																			
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-	phase1																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>phase1</td><td>Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.</td></tr><tr><td>enable</td><td>Enable forwarding auto-discovery short-cut messages.</td></tr><tr><td>disable</td><td>Disable forwarding auto-discovery short-cut messages.</td></tr></table>	Option	Description	phase1	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.	enable	Enable forwarding auto-discovery short-cut messages.	disable	Disable forwarding auto-discovery short-cut messages.											
	Option	Description																		
	phase1	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.																		
	enable	Enable forwarding auto-discovery short-cut messages.																		
disable	Disable forwarding auto-discovery short-cut messages.																			
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-	phase1																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>phase1</td><td>Send short-cut messages according to the phase1 auto-discovery-sender setting.</td></tr><tr><td>enable</td><td>Enable sending auto-discovery short-cut messages.</td></tr><tr><td>disable</td><td>Disable sending auto-discovery short-cut messages.</td></tr></table>	Option	Description	phase1	Send short-cut messages according to the phase1 auto-discovery-sender setting.	enable	Enable sending auto-discovery short-cut messages.	disable	Disable sending auto-discovery short-cut messages.											
	Option	Description																		
	phase1	Send short-cut messages according to the phase1 auto-discovery-sender setting.																		
	enable	Enable sending auto-discovery short-cut messages.																		
disable	Disable sending auto-discovery short-cut messages.																			
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.													
	Option	Description																		
	enable	Enable setting.																		
disable	Disable setting.																			
comments	Comment.	var-string	Maximum length: 255																	
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-	disable																

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																	
	Option	Description																																						
	<i>enable</i>	Enable setting.																																						
<i>disable</i>	Disable setting.																																							
dhgrp	Phase2 DH group.	option	-	14																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>DH Group 1.</td></tr><tr><td>2</td><td>DH Group 2.</td></tr><tr><td>5</td><td>DH Group 5.</td></tr><tr><td>14</td><td>DH Group 14.</td></tr><tr><td>15</td><td>DH Group 15.</td></tr><tr><td>16</td><td>DH Group 16.</td></tr><tr><td>17</td><td>DH Group 17.</td></tr><tr><td>18</td><td>DH Group 18.</td></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr><tr><td>27</td><td>DH Group 27.</td></tr><tr><td>28</td><td>DH Group 28.</td></tr><tr><td>29</td><td>DH Group 29.</td></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
	Option	Description																																						
	1	DH Group 1.																																						
	2	DH Group 2.																																						
	5	DH Group 5.																																						
	14	DH Group 14.																																						
	15	DH Group 15.																																						
	16	DH Group 16.																																						
	17	DH Group 17.																																						
	18	DH Group 18.																																						
	19	DH Group 19.																																						
	20	DH Group 20.																																						
	21	DH Group 21.																																						
	27	DH Group 27.																																						
	28	DH Group 28.																																						
	29	DH Group 29.																																						
	30	DH Group 30.																																						
	31	DH Group 31.																																						
32	DH Group 32.																																							
diffserv	Enable/disable applying DSCP value to the IPsec tunnel outer IP header.	option	-	disable																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																	
	Option	Description																																						
	<i>enable</i>	Enable setting.																																						
<i>disable</i>	Disable setting.																																							
diffservcode	DSCP value to be applied to the IPsec tunnel outer IP header.	user	Not Specified																																					
dst-addr-type	Remote proxy ID type.	option	-	subnet																																				

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>subnet</i>	IPv4 subnet.		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		
	<i>subnet6</i>	IPv6 subnet.		
	<i>range6</i>	IPv6 range.		
	<i>ip6</i>	IPv6 IP.		
	<i>name6</i>	IPv6 firewall address or group name.		
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified	::
dst-name	Remote proxy ID name.	string	Maximum length: 79	
dst-name6	Remote proxy ID name.	string	Maximum length: 79	
dst-port	Quick mode destination port (1 - 65535 or 0 for all).	integer	Minimum value: 0 0 Maximum value: 65535	
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0
dst-start-ip6	Remote proxy ID IPv6 start.	ipv6-address	Not Specified	::
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode
	Option	Description		
	<i>tunnel-mode</i>	Use tunnel mode encapsulation.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>transport-mode</i></td><td>Use transport mode encapsulation.</td></tr></table>	Option	Description	<i>transport-mode</i>	Use transport mode encapsulation.							
	Option	Description										
<i>transport-mode</i>	Use transport mode encapsulation.											
inbound-dscp-copy	Enable/disable copying of the DSCP in the ESP header to the inner IP header.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.</td></tr><tr><td><i>enable</i></td><td>Enable copying of the DSCP in the ESP header to the inner IP header.</td></tr><tr><td><i>disable</i></td><td>Disable copying of the DSCP in the ESP header to the inner IP header.</td></tr></table>	Option	Description	<i>phase1</i>	copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.	<i>enable</i>	Enable copying of the DSCP in the ESP header to the inner IP header.	<i>disable</i>	Disable copying of the DSCP in the ESP header to the inner IP header.			
	Option	Description										
	<i>phase1</i>	copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.										
	<i>enable</i>	Enable copying of the DSCP in the ESP header to the inner IP header.										
<i>disable</i>	Disable copying of the DSCP in the ESP header to the inner IP header.											
initiator-ts-narrow	Enable/disable traffic selector narrowing for IKEv2 initiator.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
keepalive	Enable/disable keep alive.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
keylife-type	Keylife type.	option	-	seconds								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>seconds</i></td><td>Key life in seconds.</td></tr><tr><td><i>kbs</i></td><td>Key life in kilobytes.</td></tr><tr><td><i>both</i></td><td>Key life both.</td></tr></table>	Option	Description	<i>seconds</i>	Key life in seconds.	<i>kbs</i>	Key life in kilobytes.	<i>both</i>	Key life both.			
	Option	Description										
	<i>seconds</i>	Key life in seconds.										
	<i>kbs</i>	Key life in kilobytes.										
<i>both</i>	Key life both.											
keylifekbs	Phase2 key life in number of kilobytes of traffic (5120 - 4294967295).	integer	Minimum value: 5120 Maximum value: 4294967295									
keylifeseconds	Phase2 key life in time in seconds (120 - 172800).	integer	Minimum value: 120 Maximum value: 172800									

Parameter	Description	Type	Size	Default
l2tp	Enable/disable L2TP over IPsec.	option	-	disable
	Option Description			
	<i>enable</i>	Enable L2TP over IPsec.		
	<i>disable</i>	Disable L2TP over IPsec.		
name	IPsec tunnel name.	string	Maximum length: 35	
pfs	Enable/disable PFS feature.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15	
proposal	Phase2 proposal.	option	-	
	Option Description			
	<i>null-md5</i>	null-md5		
	<i>null-sha1</i>	null-sha1		
	<i>null-sha256</i>	null-sha256		
	<i>null-sha384</i>	null-sha384		
	<i>null-sha512</i>	null-sha512		
	<i>des-null</i>	des-null		
	<i>des-md5</i>	des-md5		
	<i>des-sha1</i>	des-sha1		
	<i>des-sha256</i>	des-sha256		
	<i>des-sha384</i>	des-sha384		
	<i>des-sha512</i>	des-sha512		
	<i>3des-null</i>	3des-null		
	<i>3des-md5</i>	3des-md5		
	<i>3des-sha1</i>	3des-sha1		
	<i>3des-sha256</i>	3des-sha256		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>3des-sha384</i>	3des-sha384		
	<i>3des-sha512</i>	3des-sha512		
	<i>aes128-null</i>	aes128-null		
	<i>aes128-md5</i>	aes128-md5		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm</i>	aes128gcm		
	<i>aes192-null</i>	aes192-null		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-null</i>	aes256-null		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm</i>	aes256gcm		
	<i>chacha20poly1305</i>	chacha20poly1305		
	<i>aria128-null</i>	aria128-null		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		
	<i>aria128-sha512</i>	aria128-sha512		

Parameter	Description	Type	Size	Default																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria192-null</i></td><td>aria192-null</td></tr><tr><td><i>aria192-md5</i></td><td>aria192-md5</td></tr><tr><td><i>aria192-sha1</i></td><td>aria192-sha1</td></tr><tr><td><i>aria192-sha256</i></td><td>aria192-sha256</td></tr><tr><td><i>aria192-sha384</i></td><td>aria192-sha384</td></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-null</i></td><td>aria256-null</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-null</i></td><td>seed-null</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>aria192-null</i>	aria192-null	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-null</i>	aria256-null	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-null</i>	seed-null	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
	Option	Description																																								
	<i>aria192-null</i>	aria192-null																																								
	<i>aria192-md5</i>	aria192-md5																																								
	<i>aria192-sha1</i>	aria192-sha1																																								
	<i>aria192-sha256</i>	aria192-sha256																																								
	<i>aria192-sha384</i>	aria192-sha384																																								
	<i>aria192-sha512</i>	aria192-sha512																																								
	<i>aria256-null</i>	aria256-null																																								
	<i>aria256-md5</i>	aria256-md5																																								
	<i>aria256-sha1</i>	aria256-sha1																																								
	<i>aria256-sha256</i>	aria256-sha256																																								
	<i>aria256-sha384</i>	aria256-sha384																																								
	<i>aria256-sha512</i>	aria256-sha512																																								
	<i>seed-null</i>	seed-null																																								
	<i>seed-md5</i>	seed-md5																																								
	<i>seed-sha1</i>	seed-sha1																																								
	<i>seed-sha256</i>	seed-sha256																																								
	<i>seed-sha384</i>	seed-sha384																																								
<i>seed-sha512</i>	seed-sha512																																									
protocol	Quick mode protocol selector (1 - 255 or 0 for all).	integer	Minimum value: 0 0 Maximum value: 255	0																																						
replay	Enable/disable replay detection.	option	-	enable																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																			
	Option	Description																																								
	<i>enable</i>	Enable setting.																																								
<i>disable</i>	Disable setting.																																									
route-overlap	Action for overlapping routes.	option	-	use-new																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-old</i></td><td>Use the old route and do not add the new route.</td></tr></table>	Option	Description	<i>use-old</i>	Use the old route and do not add the new route.																																					
	Option	Description																																								
<i>use-old</i>	Use the old route and do not add the new route.																																									

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-new</i></td><td>Delete the old route and add the new route.</td></tr><tr><td><i>allow</i></td><td>Allow overlapping routes.</td></tr></table>	Option	Description	<i>use-new</i>	Delete the old route and add the new route.	<i>allow</i>	Allow overlapping routes.															
	Option	Description																				
	<i>use-new</i>	Delete the old route and add the new route.																				
<i>allow</i>	Allow overlapping routes.																					
single-source	Enable/disable single source IP restriction.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Only single source IP will be accepted.</td></tr><tr><td><i>disable</i></td><td>Source IP range will be accepted.</td></tr></table>	Option	Description	<i>enable</i>	Only single source IP will be accepted.	<i>disable</i>	Source IP range will be accepted.															
	Option	Description																				
	<i>enable</i>	Only single source IP will be accepted.																				
<i>disable</i>	Source IP range will be accepted.																					
src-addr-type	Local proxy ID type.	option	-	subnet																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subnet</i></td><td>IPv4 subnet.</td></tr><tr><td><i>range</i></td><td>IPv4 range.</td></tr><tr><td><i>ip</i></td><td>IPv4 IP.</td></tr><tr><td><i>name</i></td><td>IPv4 firewall address or group name.</td></tr><tr><td><i>subnet6</i></td><td>IPv6 subnet.</td></tr><tr><td><i>range6</i></td><td>IPv6 range.</td></tr><tr><td><i>ip6</i></td><td>IPv6 IP.</td></tr><tr><td><i>name6</i></td><td>IPv6 firewall address or group name.</td></tr></table>	Option	Description	<i>subnet</i>	IPv4 subnet.	<i>range</i>	IPv4 range.	<i>ip</i>	IPv4 IP.	<i>name</i>	IPv4 firewall address or group name.	<i>subnet6</i>	IPv6 subnet.	<i>range6</i>	IPv6 range.	<i>ip6</i>	IPv6 IP.	<i>name6</i>	IPv6 firewall address or group name.			
	Option	Description																				
	<i>subnet</i>	IPv4 subnet.																				
	<i>range</i>	IPv4 range.																				
	<i>ip</i>	IPv4 IP.																				
	<i>name</i>	IPv4 firewall address or group name.																				
	<i>subnet6</i>	IPv6 subnet.																				
	<i>range6</i>	IPv6 range.																				
	<i>ip6</i>	IPv6 IP.																				
<i>name6</i>	IPv6 firewall address or group name.																					
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0																		
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified	::																		
src-name	Local proxy ID name.	string	Maximum length: 79																			
src-name6	Local proxy ID name.	string	Maximum length: 79																			
src-port	Quick mode source port (1 - 65535 or 0 for all).	integer	Minimum value: 0 0 Maximum value: 65535																			

Parameter	Description	Type	Size	Default
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified	::
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0

config vpn kmip-server

KMIP server entry configuration.

```

config vpn kmip-server
  Description: KMIP server entry configuration.
  edit <name>
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set password {password}
    set server-identity-check [enable|disable]
    config server-list
      Description: KMIP server list.
      edit <id>
        set cert {string}
        set port {integer}
        set server {string}
        set status [enable|disable]
      next
    end
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set username {string}
    set vrf-select {integer}
  next
end

```

config vpn kmip-server

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default														
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.									
	Option	Description																
	auto	Set outgoing interface automatically.																
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.																
specify	Set outgoing interface manually.																	
name	KMIP server entry name.	string	Maximum length: 35															
password	Password to use for connectivity to the KMIP server.	password	Not Specified															
server-identity-check	Enable/disable KMIP server identity check (verify server FQDN/IP address against the server certificate).	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable server identity check.</td></tr><tr><td>disable</td><td>Disable server identity check.</td></tr></table>	Option	Description	enable	Enable server identity check.	disable	Disable server identity check.											
	Option	Description																
	enable	Enable server identity check.																
disable	Disable server identity check.																	
source-ip	FortiGate IP address to be used for communication with the KMIP server.	string	Maximum length: 63															
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
	Option	Description																
	default	Follow system global setting.																
	SSLv3	SSLv3.																
	TLSv1	TLSv1.																
	TLSv1-1	TLSv1.1.																
	TLSv1-2	TLSv1.2.																
TLSv1-3	TLSv1.3.																	
username	User name to use for connectivity to the KMIP server.	string	Maximum length: 63															

Parameter	Description	Type	Size	Default
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	0

config server-list

Parameter	Description	Type	Size	Default						
cert	Client certificate to use for connectivity to the KMIP server.	string	Maximum length: 35							
id	ID	integer	Minimum value: 0 0 Maximum value: 4294967295	0						
port	KMIP server port.	integer	Minimum value: 0 0 Maximum value: 65535	5696						
server	KMIP server FQDN or IP address.	string	Maximum length: 63							
status	Enable/disable KMIP server.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server.</td></tr><tr><td><i>disable</i></td><td>Disable server.</td></tr></table>				Option	Description	<i>enable</i>	Enable server.	<i>disable</i>	Disable server.
Option	Description									
<i>enable</i>	Enable server.									
<i>disable</i>	Disable server.									

config vpn l2tp

Configure L2TP.

```

config vpn l2tp
  Description: Configure L2TP.
  set compress [enable|disable]
  set eip {ipv4-address}
  set enforce-ipsec [enable|disable]
  set hello-interval {integer}
  set lcp-echo-interval {integer}
  set lcp-max-echo-fails {integer}
  set sip {ipv4-address}
  set status [enable|disable]
  set usrgrp {string}
end

```

config vpn l2tp

Parameter	Description	Type	Size	Default						
compress	Enable/disable data compression.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable compress</td></tr><tr><td><i>disable</i></td><td>Disable compress</td></tr></table>	Option	Description	<i>enable</i>	Enable compress	<i>disable</i>	Disable compress			
	Option	Description								
	<i>enable</i>	Enable compress								
<i>disable</i>	Disable compress									
eip	End IP.	ipv4-address	Not Specified	0.0.0.0						
enforce-ipsec	Enable/disable IPsec enforcement.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable enforce-ipsec</td></tr><tr><td><i>disable</i></td><td>Disable enforce-ipsec</td></tr></table>	Option	Description	<i>enable</i>	Enable enforce-ipsec	<i>disable</i>	Disable enforce-ipsec			
	Option	Description								
	<i>enable</i>	Enable enforce-ipsec								
<i>disable</i>	Disable enforce-ipsec									
hello-interval	L2TP hello message interval in seconds (0 - 3600 sec, default = 60).	integer	Minimum value: 0 Maximum value: 3600	60						
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5						
lcp-max-echo-fails	Maximum number of missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3						
sip	Start IP.	ipv4-address	Not Specified	0.0.0.0						
status	Enable/disable FortiGate as a L2TP gateway.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
usrgrp	User group.	string	Maximum length: 35							

config vpn pptp

Configure PPTP.

```
config vpn pptp
  Description: Configure PPTP.
  set eip {ipv4-address}
  set ip-mode [range|usrgrp]
  set local-ip {ipv4-address}
  set sip {ipv4-address}
  set status [enable|disable]
  set usrgrp {string}
end
```

config vpn pptp

Parameter	Description	Type	Size	Default						
eip	End IP.	ipv4-address	Not Specified	0.0.0.0						
ip-mode	IP assignment mode for PPTP client.	option	-	range						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>range</td><td>PPTP client IP from manual config (range from sip to eip).</td></tr><tr><td>usrgrp</td><td>PPTP client IP from user-group defined server.</td></tr></table>				Option	Description	range	PPTP client IP from manual config (range from sip to eip).	usrgrp	PPTP client IP from user-group defined server.
	Option	Description								
	range	PPTP client IP from manual config (range from sip to eip).								
usrgrp	PPTP client IP from user-group defined server.									
local-ip	Local IP to be used for peer's remote IP.	ipv4-address	Not Specified	0.0.0.0						
sip	Start IP.	ipv4-address	Not Specified	0.0.0.0						
status	Enable/disable FortiGate as a PPTP gateway.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									
usrgrp	User group.	string	Maximum length: 35							

config vpn qkd

Configure Quantum Key Distribution servers


```

config vpn qkd
    Description: Configure Quantum Key Distribution servers
    edit <name>
        set certificate <name1>, <name2>, ...
        set comment {var-string}
        set id {string}
        set peer {string}
        set port {integer}
        set server {string}
    next
end

```

config vpn qkd

Parameter	Description	Type	Size	Default
certificate <name>	Names of up to 4 certificates to offer to the KME. Certificate name.	string	Maximum length: 79	
comment	Comment.	var-string	Maximum length: 255	
id	Quantum Key Distribution ID assigned by the KME.	string	Maximum length: 291	
name	Quantum Key Distribution configuration name.	string	Maximum length: 35	
peer	Authenticate Quantum Key Device's certificate with the peer/peergrp.	string	Maximum length: 35	
port	Port to connect to on the KME.	integer	Minimum value: 1 Maximum value: 65535	0
server	IPv4, IPv6 or DNS address of the KME.	string	Maximum length: 63	

config vpn ssl settings



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure Agentless VPN.

```
config vpn ssl settings
  Description: Configure Agentless VPN.
  set algorithm [high|medium|...]
  set auth-session-check-source-ip [enable|disable]
  set auth-timeout {integer}
  config authentication-rule
    Description: Authentication rule for Agentless VPN.
    edit <id>
      set auth [any|local|...]
      set cipher [any|high|...]
      set client-cert [enable|disable]
      set groups <name1>, <name2>, ...
      set portal {string}
      set realm {string}
      set source-address <name1>, <name2>, ...
      set source-address-negate [enable|disable]
      set source-address6 <name1>, <name2>, ...
      set source-address6-negate [enable|disable]
      set source-interface <name1>, <name2>, ...
      set user-peer {string}
      set users <name1>, <name2>, ...
    next
  next
```

```

end
set banned-cipher {option1}, {option2}, ...
set browser-language-detection [enable|disable]
set check-referer [enable|disable]
set ciphersuite {option1}, {option2}, ...
set client-sigalgs [no-rsa-pss|all]
set default-portal {string}
set deflate-compression-level {integer}
set deflate-min-data-size {integer}
set dns-suffix {var-string}
set dtls-heartbeat-fail-count {integer}
set dtls-heartbeat-idle-timeout {integer}
set dtls-heartbeat-interval {integer}
set dtls-hello-timeout {integer}
set dual-stack-mode [enable|disable]
set encode-2f-sequence [enable|disable]
set encrypt-and-store-password [enable|disable]
set force-two-factor-auth [enable|disable]
set header-x-forwarded-for [pass|add|...]
set hsts-include-subdomains [enable|disable]
set http-compression [enable|disable]
set http-only-cookie [enable|disable]
set http-request-body-timeout {integer}
set http-request-header-timeout {integer}
set https-redirect [enable|disable]
set idle-timeout {integer}
set login-attempt-limit {integer}
set login-block-time {integer}
set login-timeout {integer}
set port {integer}
set port-precedence [enable|disable]
set reqclientcert [enable|disable]
set server-hostname {string}
set servercert {string}
set source-address <name1>, <name2>, ...
set source-address-negate [enable|disable]
set source-address6 <name1>, <name2>, ...
set source-address6-negate [enable|disable]
set source-interface <name1>, <name2>, ...
set ssl-client-renegotiation [disable|enable]
set ssl-insert-empty-fragment [enable|disable]
set ssl-max-proto-ver [tls1-0|tls1-1|...]
set ssl-min-proto-ver [tls1-0|tls1-1|...]
set status [enable|disable]
set transform-backward-slashes [enable|disable]
set unsafe-legacy-renegotiation [enable|disable]
set url-obscuration [enable|disable]
set user-peer {string}
set x-content-type-options [enable|disable]
end

```

config vpn ssl settings

Parameter	Description	Type	Size	Default																
algorithm	Force the Agentless VPN security level. High allows only high. Medium allows medium and high. Low allows any.	option	-	high																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High algorithms.</td></tr><tr><td>medium</td><td>High and medium algorithms.</td></tr><tr><td>default</td><td>default</td></tr><tr><td>low</td><td>All algorithms.</td></tr></table>	Option	Description	high	High algorithms.	medium	High and medium algorithms.	default	default	low	All algorithms.									
Option	Description																			
high	High algorithms.																			
medium	High and medium algorithms.																			
default	default																			
low	All algorithms.																			
auth-session-check-source-ip	Enable/disable checking of source IP for authentication session.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable checking of source IP for authentication session.</td></tr><tr><td>disable</td><td>Disable checking of source IP for authentication session.</td></tr></table>	Option	Description	enable	Enable checking of source IP for authentication session.	disable	Disable checking of source IP for authentication session.													
Option	Description																			
enable	Enable checking of source IP for authentication session.																			
disable	Disable checking of source IP for authentication session.																			
auth-timeout	Agentless VPN authentication timeout (1 - 259200 sec (3 days), 0 for no timeout).	integer	Minimum value: 0 Maximum value: 259200	28800																
banned-cipher	Select one or more cipher technologies that cannot be used in Agentless VPN negotiations. Only applies to TLS 1.2 and below.	option	-	SHA1 SHA256 SHA384																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>RSA</td><td>Ban the use of cipher suites using RSA key.</td></tr><tr><td>DHE</td><td>Ban the use of cipher suites using authenticated ephemeral DH key agreement.</td></tr><tr><td>ECDHE</td><td>Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.</td></tr><tr><td>DSS</td><td>Ban the use of cipher suites using DSS authentication.</td></tr><tr><td>ECDSA</td><td>Ban the use of cipher suites using ECDSA authentication.</td></tr><tr><td>AES</td><td>Ban the use of cipher suites using either 128 or 256 bit AES.</td></tr><tr><td>AESGCM</td><td>Ban the use of cipher suites AES in Galois Counter Mode (GCM).</td></tr></table>	Option	Description	RSA	Ban the use of cipher suites using RSA key.	DHE	Ban the use of cipher suites using authenticated ephemeral DH key agreement.	ECDHE	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.	DSS	Ban the use of cipher suites using DSS authentication.	ECDSA	Ban the use of cipher suites using ECDSA authentication.	AES	Ban the use of cipher suites using either 128 or 256 bit AES.	AESGCM	Ban the use of cipher suites AES in Galois Counter Mode (GCM).			
Option	Description																			
RSA	Ban the use of cipher suites using RSA key.																			
DHE	Ban the use of cipher suites using authenticated ephemeral DH key agreement.																			
ECDHE	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.																			
DSS	Ban the use of cipher suites using DSS authentication.																			
ECDSA	Ban the use of cipher suites using ECDSA authentication.																			
AES	Ban the use of cipher suites using either 128 or 256 bit AES.																			
AESGCM	Ban the use of cipher suites AES in Galois Counter Mode (GCM).																			

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>CAMELLIA</td><td>Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.</td></tr><tr><td>3DES</td><td>Ban the use of cipher suites using triple DES</td></tr><tr><td>SHA1</td><td>Ban the use of cipher suites using HMAC-SHA1.</td></tr><tr><td>SHA256</td><td>Ban the use of cipher suites using HMAC-SHA256.</td></tr><tr><td>SHA384</td><td>Ban the use of cipher suites using HMAC-SHA384.</td></tr><tr><td>STATIC</td><td>Ban the use of cipher suites using static keys.</td></tr><tr><td>CHACHA20</td><td>Ban the use of cipher suites using ChaCha20.</td></tr><tr><td>ARIA</td><td>Ban the use of cipher suites using ARIA.</td></tr><tr><td>AESCCM</td><td>Ban the use of cipher suites using AESCCM.</td></tr></table>	Option	Description	CAMELLIA	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.	3DES	Ban the use of cipher suites using triple DES	SHA1	Ban the use of cipher suites using HMAC-SHA1.	SHA256	Ban the use of cipher suites using HMAC-SHA256.	SHA384	Ban the use of cipher suites using HMAC-SHA384.	STATIC	Ban the use of cipher suites using static keys.	CHACHA20	Ban the use of cipher suites using ChaCha20.	ARIA	Ban the use of cipher suites using ARIA.	AESCCM	Ban the use of cipher suites using AESCCM.			
	Option	Description																						
	CAMELLIA	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.																						
	3DES	Ban the use of cipher suites using triple DES																						
	SHA1	Ban the use of cipher suites using HMAC-SHA1.																						
	SHA256	Ban the use of cipher suites using HMAC-SHA256.																						
	SHA384	Ban the use of cipher suites using HMAC-SHA384.																						
	STATIC	Ban the use of cipher suites using static keys.																						
	CHACHA20	Ban the use of cipher suites using ChaCha20.																						
	ARIA	Ban the use of cipher suites using ARIA.																						
AESCCM	Ban the use of cipher suites using AESCCM.																							
browser-language-detection	Enable/disable overriding the configured system language based on the preferred language of the browser.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.																	
	Option	Description																						
	enable	Enable setting.																						
disable	Disable setting.																							
check-referer	Enable/disable verification of referer field in HTTP request header.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable verification of referer field in HTTP request header.</td></tr><tr><td>disable</td><td>Disable verification of referer field in HTTP request header.</td></tr></table>	Option	Description	enable	Enable verification of referer field in HTTP request header.	disable	Disable verification of referer field in HTTP request header.																	
	Option	Description																						
	enable	Enable verification of referer field in HTTP request header.																						
disable	Disable verification of referer field in HTTP request header.																							
ciphersuite	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, set ssl-max-proto-ver to tls1-2 or below.	option	-	TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-AES-128-GCM-SHA256</td><td>Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.</td></tr></table>	Option	Description	TLS-AES-128-GCM-SHA256	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.																			
	Option	Description																						
TLS-AES-128-GCM-SHA256	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.																							

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-AES-256-GCM-SHA384</i></td><td>Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.</td></tr><tr><td><i>TLS-CHACHA20-POLY1305-SHA256</i></td><td>Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.</td></tr><tr><td><i>TLS-AES-128-CCM-SHA256</i></td><td>Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.</td></tr><tr><td><i>TLS-AES-128-CCM-8-SHA256</i></td><td>Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.</td></tr></table>	Option	Description	<i>TLS-AES-256-GCM-SHA384</i>	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.	<i>TLS-AES-128-CCM-SHA256</i>	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.	<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.			
	Option	Description												
	<i>TLS-AES-256-GCM-SHA384</i>	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.												
	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.												
	<i>TLS-AES-128-CCM-SHA256</i>	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.												
<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.													
client-sigalgs	Set signature algorithms related to client authentication. Affects TLS version <= 1.2 only.	option	-	all										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-rsa-pss</i></td><td>Disable RSA-PSS signature algorithms for client authentication.</td></tr><tr><td><i>all</i></td><td>Enable all supported signature algorithms for client authentication.</td></tr></table>	Option	Description	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for client authentication.	<i>all</i>	Enable all supported signature algorithms for client authentication.							
	Option	Description												
	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for client authentication.												
<i>all</i>	Enable all supported signature algorithms for client authentication.													
default-portal	Default Agentless VPN portal.	string	Maximum length: 35											
deflate-compression-level	Compression level (0~9).	integer	Minimum value: 0 Maximum value: 9	6										
deflate-min-data-size	Minimum amount of data that triggers compression (200 - 65535 bytes).	integer	Minimum value: 200 Maximum value: 65535	300										
dns-suffix	DNS suffix used for Agentless VPN clients.	var-string	Maximum length: 253											
dtls-heartbeat-fail-count	Number of missing heartbeats before the connection is considered dropped.	integer	Minimum value: 3 Maximum value: 10	3										
dtls-heartbeat-idle-timeout	Idle timeout before DTLS heartbeat is sent.	integer	Minimum value: 3 Maximum value: 10	3										
dtls-heartbeat-interval	Interval between DTLS heartbeat.	integer	Minimum value: 3 Maximum value: 10	3										

Parameter	Description	Type	Size	Default								
dtls-hello-timeout	SSLVPN maximum DTLS hello timeout (10 - 60 sec, default = 10).	integer	Minimum value: 10 Maximum value: 60	10								
dual-stack-mode	Agentless web mode: support IPv4 and IPv6 bookmarks in the portal.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
encode-2f-sequence	Encode \2F sequence to forward slash in URLs.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
encrypt-and-store-password	Encrypt and store user passwords for Agentless VPN web sessions.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
force-two-factor-auth	Enable/disable only PKI users with two-factor authentication for Agentless VPNs.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
header-x-forwarded-for	Forward the same, add, or remove HTTP header.	option	-	add								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
hsts-include-subdomains	Add HSTS includeSubDomains response header.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
http-compression	Enable/disable to allow HTTP compression over Agentless VPN connections.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
http-only-cookie	Enable/disable Agentless VPN support for HttpOnly cookies.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
http-request-body-timeout	Agentless VPN session is disconnected if an HTTP request body is not received within this time (1 - 60 sec, default = 20).	integer	Minimum value: 0 Maximum value: 4294967295	30
http-request-header-timeout	Agentless VPN session is disconnected if an HTTP request header is not received within this time (1 - 60 sec, default = 20).	integer	Minimum value: 0 Maximum value: 4294967295	20
https-redirect	Enable/disable redirect of port 80 to Agentless VPN port.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
idle-timeout	Agentless VPN disconnects if idle for specified time in seconds.	integer	Minimum value: 0 Maximum value: 259200	300
login-attempt-limit	Agentless VPN maximum login attempt times before block (0 - 10, default = 2, 0 = no limit).	integer	Minimum value: 0 Maximum value: 10	2

Parameter	Description	Type	Size	Default
login-block-time	Time for which a user is blocked from logging in after too many failed login attempts (0 - 86400 sec, default = 60).	integer	Minimum value: 0 Maximum value: 86400	60
login-timeout	Agentless VPN maximum login timeout (10 - 180 sec, default = 30).	integer	Minimum value: 10 Maximum value: 180	30
port	Agentless VPN access port (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	10443
port-precedence	Enable/disable, Enable means that if Agentless VPN connections are allowed on an interface admin GUI connections are blocked on that interface.	option	-	enable
	Option		Description	
	enable		Enable setting.	
	disable		Disable setting.	
reqclientcert	Enable/disable to require client certificates for all Agentless VPN users.	option	-	disable
	Option		Description	
	enable		Enable setting.	
	disable		Disable setting.	
server-hostname	Server hostname for HTTPS. When set, will be used for Agentless VPN web proxy host header for any redirection.	string	Maximum length: 255	
servercert	Name of the server certificate to be used for Agentless VPNs.	string	Maximum length: 35	
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79	
source-address-negate	Enable/disable negated source address match.	option	-	disable
	Option		Description	
	enable		Enable setting.	
	disable		Disable setting.	

Parameter	Description	Type	Size	Default										
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79											
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
source-interface <name>	Agentless VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35											
ssl-client-renegotiation	Enable/disable to allow client renegotiation by the server if the tunnel goes down.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Abort any SSL connection that attempts to renegotiate.</td></tr><tr><td><i>enable</i></td><td>Allow a SSL client to renegotiate.</td></tr></table>	Option	Description	<i>disable</i>	Abort any SSL connection that attempts to renegotiate.	<i>enable</i>	Allow a SSL client to renegotiate.							
Option	Description													
<i>disable</i>	Abort any SSL connection that attempts to renegotiate.													
<i>enable</i>	Allow a SSL client to renegotiate.													
ssl-insert-empty-fragment	Enable/disable insertion of empty fragment.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
ssl-max-protocol-ver	SSL maximum protocol version.	option	-	tls1-3										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls1-0</i></td><td>TLS version 1.0.</td></tr><tr><td><i>tls1-1</i></td><td>TLS version 1.1.</td></tr><tr><td><i>tls1-2</i></td><td>TLS version 1.2.</td></tr><tr><td><i>tls1-3</i></td><td>TLS version 1.3.</td></tr></table>	Option	Description	<i>tls1-0</i>	TLS version 1.0.	<i>tls1-1</i>	TLS version 1.1.	<i>tls1-2</i>	TLS version 1.2.	<i>tls1-3</i>	TLS version 1.3.			
Option	Description													
<i>tls1-0</i>	TLS version 1.0.													
<i>tls1-1</i>	TLS version 1.1.													
<i>tls1-2</i>	TLS version 1.2.													
<i>tls1-3</i>	TLS version 1.3.													
ssl-min-protocol-ver	SSL minimum protocol version.	option	-	tls1-2										

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls1-0</i></td><td>TLS version 1.0.</td></tr><tr><td><i>tls1-1</i></td><td>TLS version 1.1.</td></tr><tr><td><i>tls1-2</i></td><td>TLS version 1.2.</td></tr><tr><td><i>tls1-3</i></td><td>TLS version 1.3.</td></tr></table>	Option	Description	<i>tls1-0</i>	TLS version 1.0.	<i>tls1-1</i>	TLS version 1.1.	<i>tls1-2</i>	TLS version 1.2.	<i>tls1-3</i>	TLS version 1.3.			
	Option	Description												
	<i>tls1-0</i>	TLS version 1.0.												
	<i>tls1-1</i>	TLS version 1.1.												
	<i>tls1-2</i>	TLS version 1.2.												
<i>tls1-3</i>	TLS version 1.3.													
status	Enable/disable Agentless VPN.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Agentless VPN.</td></tr><tr><td><i>disable</i></td><td>Disable Agentless VPN.</td></tr></table>	Option	Description	<i>enable</i>	Enable Agentless VPN.	<i>disable</i>	Disable Agentless VPN.							
	Option	Description												
	<i>enable</i>	Enable Agentless VPN.												
<i>disable</i>	Disable Agentless VPN.													
transform-backward-slashes	Transform backward slashes to forward slashes in URLs.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
unsafe-legacy-renegotiation	Enable/disable unsafe legacy re-negotiation.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
url-obscuration	Enable/disable to obscure the host name of the URL of the web browser display.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
user-peer	Name of user peer.	string	Maximum length: 35											
x-content-type-options	Add HTTP X-Content-Type-Options header.	option	-	enable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config authentication-rule

Parameter	Description	Type	Size	Default
auth	Agentless VPN authentication method restriction.	option	-	any
	Option	Description		
	<i>any</i>	Any		
	<i>local</i>	Local		
	<i>radius</i>	RADIUS		
	<i>tacacs+</i>	TACACS+		
	<i>ldap</i>	LDAP		
	<i>peer</i>	PEER		
cipher	Agentless VPN cipher strength.	option	-	high
	Option	Description		
	<i>any</i>	Any cipher strength.		
	<i>high</i>	High cipher strength (>= 168 bits).		
	<i>medium</i>	Medium cipher strength (>= 128 bits).		
client-cert	Enable/disable Agentless VPN client certificate restrictive.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
groups <name>	User groups. Group name.	string	Maximum length: 79	
id	ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default						
portal	Agentless VPN portal.	string	Maximum length: 35							
realm	Agentless VPN realm.	string	Maximum length: 35							
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79							
source-address-negate	Enable/disable negated source address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79							
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
source-interface <name>	Agentless VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35							
user-peer	Name of user peer.	string	Maximum length: 35							
users <name>	User name. User name.	string	Maximum length: 79							

config vpn ssl web portal



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Portal.

```
config vpn ssl web portal
  Description: Portal.
  edit <name>
    set allow-user-access {option1}, {option2}, ...
    config bookmark-group
      Description: Portal bookmark group.
      edit <name>
        config bookmarks
          Description: Bookmark table.
          edit <name>
            set additional-params {var-string}
            set apptype [ftp|rdp|...]
            set color-depth [32|16|...]
            set description {var-string}
            set domain {var-string}
            set folder {var-string}
            config form-data
              Description: Form data.
              edit <name>
                set value {var-string}
              next
            end
          end
        end
      end
    end
  end
```

```

        set height {integer}
        set host {var-string}
        set keyboard-layout [ar-101|ar-102|...]
        set load-balancing-info {var-string}
        set logon-password {password}
        set logon-user {var-string}
        set port {integer}
        set preconnection-blob {var-string}
        set preconnection-id {integer}
        set restricted-admin [enable|disable]
        set security [any|rdp|...]
        set send-preconnection-id [enable|disable]
        set sso [disable|static|...]
        set sso-credential [sslvpn-login|alternative]
        set sso-credential-sent-once [enable|disable]
        set sso-password {password}
        set sso-username {var-string}
        set url {var-string}
        set vnc-keyboard-layout [default|da|...]
        set width {integer}
    next
end
next
end
set clipboard [enable|disable]
set custom-lang {string}
set customize-forticlient-download-url [enable|disable]
set default-protocol [web|ftp|...]
set default-window-height {integer}
set default-window-width {integer}
set display-bookmark [enable|disable]
set display-connection-tools [enable|disable]
set display-history [enable|disable]
set display-status [enable|disable]
set dns-suffix {var-string}
set focus-bookmark [enable|disable]
set forticlient-download [enable|disable]
set forticlient-download-method [direct|ssl-vpn]
set heading {string}
set hide-sso-credential [enable|disable]
config landing-page
    Description: Landing page options.
    config form-data
        Description: Form data.
        edit <name>
            set value {var-string}
        next
    end
    set sso [disable|static|...]
    set sso-credential [sslvpn-login|alternative]
    set sso-password {password}
    set sso-username {var-string}

```

```

        set url {var-string}
    end
    set landing-page-mode [enable|disable]
    set limit-user-logins [enable|disable]
    set macos-forticlient-download-url {var-string}
    set prefer-ipv6-dns [enable|disable]
    set redir-url {var-string}
    set rewrite-ip-uri-ui [enable|disable]
    set smb-max-version [smbv1|smbv2|...]
    set smb-min-version [smbv1|smbv2|...]
    set smb-ntlmv1-auth [enable|disable]
    set smbv1 [enable|disable]
    set theme [jade|neutrino|...]
    set use-sdwan [enable|disable]
    set user-bookmark [enable|disable]
    set user-group-bookmark [enable|disable]
    set web-mode [enable|disable]
    set windows-forticlient-download-url {var-string}
next
end

```

config vpn ssl web portal

Parameter	Description	Type	Size	Default
allow-user-access	Allow user access to Agentless VPN applications.	option	-	web ftp smb sftp telnet ssh vnc rdp ping
	Option	Description		
	web	HTTP/HTTPS access.		
	ftp	FTP access.		
	smb	SMB/CIFS access.		
	sftp	SFTP access.		
	telnet	TELNET access.		
	ssh	SSH access.		
	vnc	VNC access.		
	rdp	RDP access.		
	ping	PING access.		
clipboard	Enable to support RDP/VPC clipboard functionality.	option	-	enable

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support of RDP/VNC clipboard.</td></tr><tr><td><i>disable</i></td><td>Disable support of RDP/VNC clipboard.</td></tr></table>	Option	Description	<i>enable</i>	Enable support of RDP/VNC clipboard.	<i>disable</i>	Disable support of RDP/VNC clipboard.															
	Option	Description																				
	<i>enable</i>	Enable support of RDP/VNC clipboard.																				
<i>disable</i>	Disable support of RDP/VNC clipboard.																					
custom-lang	Change the web portal display language. Overrides config system global set language. You can use config system custom-language and execute system custom-language to add custom language files.	string	Maximum length: 35																			
customize-forticlient-download-url	Enable support of customized download URL for FortiClient.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
	Option	Description																				
	<i>enable</i>	Enable setting.																				
<i>disable</i>	Disable setting.																					
default-protocol	Application type that is set by default.	option	-	web																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>web</i></td><td>HTTP/HTTPS.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>telnet</i></td><td>Telnet.</td></tr><tr><td><i>smb</i></td><td>SMB/CIFS.</td></tr><tr><td><i>vnc</i></td><td>VNC.</td></tr><tr><td><i>rdp</i></td><td>RDP.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr></table>	Option	Description	<i>web</i>	HTTP/HTTPS.	<i>ftp</i>	FTP.	<i>telnet</i>	Telnet.	<i>smb</i>	SMB/CIFS.	<i>vnc</i>	VNC.	<i>rdp</i>	RDP.	<i>ssh</i>	SSH.	<i>sftp</i>	SFTP.			
	Option	Description																				
	<i>web</i>	HTTP/HTTPS.																				
	<i>ftp</i>	FTP.																				
	<i>telnet</i>	Telnet.																				
	<i>smb</i>	SMB/CIFS.																				
	<i>vnc</i>	VNC.																				
	<i>rdp</i>	RDP.																				
<i>ssh</i>	SSH.																					
<i>sftp</i>	SFTP.																					
default-window-height	Screen height (range from 0 - 65535, default = 768).	integer	Minimum value: 0 Maximum value: 65535	768																		

Parameter	Description	Type	Size	Default						
default-window-width	Screen width (range from 0 - 65535, default = 1024).	integer	Minimum value: 0 Maximum value: 65535	1024						
display-bookmark	Enable to display the web portal bookmark widget.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
display-connection-tools	Enable to display the web portal connection tools widget.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
display-history	Enable to display the web portal user login history widget.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
display-status	Enable to display the web portal status widget.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
dns-suffix	DNS suffix.	var-string	Maximum length: 253							
focus-bookmark	Enable to prioritize the placement of the bookmark section over the quick-connection section in the Agentless VPN application.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr></table>	Option	Description	enable	Enable setting.					
Option	Description									
enable	Enable setting.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable setting.		
	<i>enable</i>	Enable setting.		
forticlient-download	Enable/disable download option for FortiClient.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
forticlient-download-method	FortiClient download method.	option	-	direct
	Option	Description		
	<i>direct</i>	Download via direct link.		
	<i>ssl-vpn</i>	Download via Agentless VPN.		
heading	Web portal heading message.	string	Maximum length: 31	Agentless VPN Portal
hide-sso-credential	Enable to prevent SSO credential being sent to client.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
landing-page-mode	Enable/disable Agentless VPN landing page mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
limit-user-logins	Enable to limit each user to one Agentless VPN session at a time.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default								
macos-forticlient-download-url	Download URL for Mac FortiClient.	var-string	Maximum length: 1023									
name	Portal name.	string	Maximum length: 35									
prefer-ipv6-dns	Prefer to query IPv6 DNS server first if enabled.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.		
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
redir-url	Client login redirect URL.	var-string	Maximum length: 255									
rewrite-ip-uri-ui	Rewrite contents for URI contains IP and /ui/ (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable contents rewrite for URI contains "IP-address/ui/".</td></tr><tr><td>disable</td><td>Disable contents rewrite for URI contains "IP-address/ui/".</td></tr></table>				Option	Description	enable	Enable contents rewrite for URI contains "IP-address/ui/".	disable	Disable contents rewrite for URI contains "IP-address/ui/".		
	Option	Description										
	enable	Enable contents rewrite for URI contains "IP-address/ui/".										
disable	Disable contents rewrite for URI contains "IP-address/ui/".											
smb-max-version	SMB maximum client protocol version.	option	-	smbv3								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>smbv1</td><td>SMB version 1.</td></tr><tr><td>smbv2</td><td>SMB version 2.</td></tr><tr><td>smbv3</td><td>SMB version 3.</td></tr></table>				Option	Description	smbv1	SMB version 1.	smbv2	SMB version 2.	smbv3	SMB version 3.
	Option	Description										
	smbv1	SMB version 1.										
	smbv2	SMB version 2.										
smbv3	SMB version 3.											
smb-min-version	SMB minimum client protocol version.	option	-	smbv2								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>smbv1</td><td>SMB version 1.</td></tr><tr><td>smbv2</td><td>SMB version 2.</td></tr><tr><td>smbv3</td><td>SMB version 3.</td></tr></table>				Option	Description	smbv1	SMB version 1.	smbv2	SMB version 2.	smbv3	SMB version 3.
	Option	Description										
	smbv1	SMB version 1.										
	smbv2	SMB version 2.										
smbv3	SMB version 3.											
smb-ntlmv1-auth	Enable support of NTLMv1 for Samba authentication.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
smbv1	SMB version 1.	option	-	disable
	Option	Description		
	<i>enable</i>	enable		
	<i>disable</i>	disable		
theme	Web portal color scheme.	option	-	security-fabric
	Option	Description		
	<i>jade</i>	Jade theme.		
	<i>neutrino</i>	Neutrino theme.		
	<i>mariner</i>	Mariner theme.		
	<i>graphite</i>	Graphite theme.		
	<i>melongene</i>	Melongene theme.		
	<i>jet-stream</i>	Jet Stream theme.		
	<i>security-fabric</i>	Security Fabric theme.		
	<i>dark-matter</i>	Dark Matter theme.		
	<i>onyx</i>	Onyx theme.		
	<i>eclipse</i>	Eclipse theme.		
use-sdwan	Use SD-WAN rules to get output interface.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
user-bookmark	Enable to allow web portal users to create their own bookmarks.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
user-group-bookmark	Enable to allow web portal users to create bookmarks for all users in the same user group.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-mode	Enable/disable Agentless VPN web mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
windows-forticlient-download-url	Download URL for Windows FortiClient.	var-string	Maximum length: 1023	

config bookmark-group

Parameter	Description	Type	Size	Default
name	Bookmark group name.	string	Maximum length: 35	

config bookmarks

Parameter	Description	Type	Size	Default
additional-params	Additional parameters.	var-string	Maximum length: 128	
apptype	Application type.	option	-	web
	Option	Description		
	<i>ftp</i>	FTP.		
	<i>rdp</i>	RDP.		
	<i>sftp</i>	SFTP.		
	<i>smb</i>	SMB/CIFS.		
	<i>ssh</i>	SSH.		
	<i>telnet</i>	Telnet.		
	<i>vnc</i>	VNC.		

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>web</td><td>HTTP/HTTPS.</td></tr></table>	Option	Description	web	HTTP/HTTPS.																							
	Option	Description																										
web	HTTP/HTTPS.																											
color-depth	Color depth per pixel.	option	-	16																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>32</td><td>32bits per pixel.</td></tr><tr><td>16</td><td>16bits per pixel.</td></tr><tr><td>8</td><td>8bits per pixel.</td></tr></table>	Option	Description	32	32bits per pixel.	16	16bits per pixel.	8	8bits per pixel.																			
	Option	Description																										
	32	32bits per pixel.																										
	16	16bits per pixel.																										
8	8bits per pixel.																											
description	Description.	var-string	Maximum length: 128																									
domain	Login domain.	var-string	Maximum length: 128																									
folder	Network shared file folder parameter.	var-string	Maximum length: 128																									
height	Screen height (range from 0 - 65535, default = 0).	integer	Minimum value: 0 0 Maximum value: 65535																									
host	Host name/IP parameter.	var-string	Maximum length: 128																									
keyboard-layout	Keyboard layout.	option	-	en-us																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ar-101</td><td>Arabic (101).</td></tr><tr><td>ar-102</td><td>Arabic (102).</td></tr><tr><td>ar-102-azerty</td><td>Arabic (102) AZERTY.</td></tr><tr><td>can-mul</td><td>Canadian Multilingual Standard.</td></tr><tr><td>cz</td><td>Czech.</td></tr><tr><td>cz-qwerty</td><td>Czech (QWERTY).</td></tr><tr><td>cz-pr</td><td>Czech Programmers.</td></tr><tr><td>da</td><td>Danish.</td></tr><tr><td>nl</td><td>Dutch.</td></tr><tr><td>de</td><td>German.</td></tr><tr><td>de-ch</td><td>German, Switzerland.</td></tr></table>	Option	Description	ar-101	Arabic (101).	ar-102	Arabic (102).	ar-102-azerty	Arabic (102) AZERTY.	can-mul	Canadian Multilingual Standard.	cz	Czech.	cz-qwerty	Czech (QWERTY).	cz-pr	Czech Programmers.	da	Danish.	nl	Dutch.	de	German.	de-ch	German, Switzerland.			
	Option	Description																										
	ar-101	Arabic (101).																										
	ar-102	Arabic (102).																										
	ar-102-azerty	Arabic (102) AZERTY.																										
	can-mul	Canadian Multilingual Standard.																										
	cz	Czech.																										
	cz-qwerty	Czech (QWERTY).																										
	cz-pr	Czech Programmers.																										
	da	Danish.																										
	nl	Dutch.																										
	de	German.																										
de-ch	German, Switzerland.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finnish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-apple</i>	French, Apple.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgium.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ja-106</i>	Japanese 106/109 key.		
	<i>ko</i>	Korean.		
	<i>la-am</i>	Latin American.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		
	<i>lt-std</i>	Lithuanian Standard.		
	<i>lav-std</i>	Latvian (Standard).		
	<i>lav-leg</i>	Latvian (Legacy).		
	<i>mk</i>	Macedonian (FYROM).		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mk-std</i>	Macedonia (FYROM) - Standard.		
	<i>no</i>	Norwegian.		
	<i>no-sami</i>	Norwegian with Sami.		
	<i>pol-214</i>	Polish (214).		
	<i>pol-pr</i>	Polish (Programmers).		
	<i>pt</i>	Portuguese.		
	<i>pt-br</i>	Portuguese (Brazilian ABNT).		
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).		
	<i>ru</i>	Russian.		
	<i>ru-mne</i>	Russian - Mnemonic.		
	<i>ru-t</i>	Russian (Typewriter).		
	<i>sl</i>	Slovenian.		
	<i>sv</i>	Swedish.		
	<i>sv-sami</i>	Swedish with Sami.		
	<i>tuk</i>	Turkmen.		
	<i>tur-f</i>	Turkish F.		
	<i>tur-q</i>	Turkish Q.		
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.		
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.		
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).		
	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.		
	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.		
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511	
logon-password	Logon password.	password	Not Specified	
logon-user	Logon user.	var-string	Maximum length: 35	
name	Bookmark name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default										
port	Remote port.	integer	Minimum value: 0 0 Maximum value: 65535	0										
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511											
preconnection-id	The numeric ID of the RDP source (0-4294967295).	integer	Minimum value: 0 0 Maximum value: 4294967295	0										
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable restricted admin mode for RDP.</td></tr><tr><td><i>disable</i></td><td>Disable restricted admin mode for RDP.</td></tr></table>	Option	Description	<i>enable</i>	Enable restricted admin mode for RDP.	<i>disable</i>	Disable restricted admin mode for RDP.							
Option	Description													
<i>enable</i>	Enable restricted admin mode for RDP.													
<i>disable</i>	Disable restricted admin mode for RDP.													
security	Security mode for RDP connection (default = any).	option	-	any										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Allow the server to choose the type of security.</td></tr><tr><td><i>rdp</i></td><td>Standard RDP encryption.</td></tr><tr><td><i>nla</i></td><td>Network Level Authentication.</td></tr><tr><td><i>tls</i></td><td>TLS encryption.</td></tr></table>	Option	Description	<i>any</i>	Allow the server to choose the type of security.	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.			
Option	Description													
<i>any</i>	Allow the server to choose the type of security.													
<i>rdp</i>	Standard RDP encryption.													
<i>nla</i>	Network Level Authentication.													
<i>tls</i>	TLS encryption.													
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of preconnection ID.</td></tr><tr><td><i>disable</i></td><td>Disable sending of preconnection ID.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of preconnection ID.	<i>disable</i>	Disable sending of preconnection ID.							
Option	Description													
<i>enable</i>	Enable sending of preconnection ID.													
<i>disable</i>	Disable sending of preconnection ID.													
sso	Single sign-on.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSO.</td></tr><tr><td><i>static</i></td><td>Static SSO.</td></tr><tr><td><i>auto</i></td><td>Auto SSO.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSO.	<i>static</i>	Static SSO.	<i>auto</i>	Auto SSO.					
Option	Description													
<i>disable</i>	Disable SSO.													
<i>static</i>	Static SSO.													
<i>auto</i>	Auto SSO.													

Parameter	Description	Type	Size	Default																										
sso-credential	Single sign-on credentials.	option	-	sslvpn-login																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sslvpn-login</td><td>Agentless VPN login.</td></tr><tr><td>alternative</td><td>Alternative.</td></tr></table>	Option	Description	sslvpn-login	Agentless VPN login.	alternative	Alternative.																							
	Option	Description																												
	sslvpn-login	Agentless VPN login.																												
alternative	Alternative.																													
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Single sign-on credentials are only sent once to remote server.</td></tr><tr><td>disable</td><td>Single sign-on credentials are sent to remote server for every HTTP request.</td></tr></table>	Option	Description	enable	Single sign-on credentials are only sent once to remote server.	disable	Single sign-on credentials are sent to remote server for every HTTP request.																							
	Option	Description																												
	enable	Single sign-on credentials are only sent once to remote server.																												
disable	Single sign-on credentials are sent to remote server for every HTTP request.																													
sso-password	SSO password.	password	Not Specified																											
sso-username	SSO user name.	var-string	Maximum length: 35																											
url	URL parameter.	var-string	Maximum length: 128																											
vnc-keyboard-layout	Keyboard layout.	option	-	default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Default.</td></tr><tr><td>da</td><td>Danish.</td></tr><tr><td>nl</td><td>Dutch.</td></tr><tr><td>en-uk</td><td>English, United Kingdom.</td></tr><tr><td>en-uk-ext</td><td>English, United Kingdom Extended.</td></tr><tr><td>fi</td><td>Finnish.</td></tr><tr><td>fr</td><td>French.</td></tr><tr><td>fr-be</td><td>French, Belgium.</td></tr><tr><td>fr-ca-mul</td><td>French, Canadian Multilingual Std.</td></tr><tr><td>de</td><td>German.</td></tr><tr><td>de-ch</td><td>German, Switzerland.</td></tr><tr><td>it</td><td>Italian.</td></tr></table>	Option	Description	default	Default.	da	Danish.	nl	Dutch.	en-uk	English, United Kingdom.	en-uk-ext	English, United Kingdom Extended.	fi	Finnish.	fr	French.	fr-be	French, Belgium.	fr-ca-mul	French, Canadian Multilingual Std.	de	German.	de-ch	German, Switzerland.	it	Italian.			
	Option	Description																												
	default	Default.																												
	da	Danish.																												
	nl	Dutch.																												
	en-uk	English, United Kingdom.																												
	en-uk-ext	English, United Kingdom Extended.																												
	fi	Finnish.																												
	fr	French.																												
	fr-be	French, Belgium.																												
	fr-ca-mul	French, Canadian Multilingual Std.																												
	de	German.																												
	de-ch	German, Switzerland.																												
it	Italian.																													

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>it-142</i></td><td>Italian (142).</td></tr><tr><td><i>pt</i></td><td>Portuguese.</td></tr><tr><td><i>pt-br-abnt2</i></td><td>Portuguese (Brazilian ABNT2).</td></tr><tr><td><i>no</i></td><td>Norwegian.</td></tr><tr><td><i>gd</i></td><td>Scottish Gaelic.</td></tr><tr><td><i>es</i></td><td>Spanish.</td></tr><tr><td><i>sv</i></td><td>Swedish.</td></tr><tr><td><i>us-intl</i></td><td>United States-International.</td></tr></table>	Option	Description	<i>it-142</i>	Italian (142).	<i>pt</i>	Portuguese.	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).	<i>no</i>	Norwegian.	<i>gd</i>	Scottish Gaelic.	<i>es</i>	Spanish.	<i>sv</i>	Swedish.	<i>us-intl</i>	United States-International.			
	Option	Description																				
	<i>it-142</i>	Italian (142).																				
	<i>pt</i>	Portuguese.																				
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).																				
	<i>no</i>	Norwegian.																				
	<i>gd</i>	Scottish Gaelic.																				
	<i>es</i>	Spanish.																				
	<i>sv</i>	Swedish.																				
<i>us-intl</i>	United States-International.																					
width	Screen width (range from 0 - 65535, default = 0).	integer	Minimum value: 0 0 Maximum value: 65535																			

config form-data

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

config landing-page

Parameter	Description	Type	Size	Default								
sso	Single sign-on.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSO.</td></tr><tr><td><i>static</i></td><td>Static SSO.</td></tr><tr><td><i>auto</i></td><td>Auto SSO.</td></tr></table>				Option	Description	<i>disable</i>	Disable SSO.	<i>static</i>	Static SSO.	<i>auto</i>	Auto SSO.
	Option	Description										
	<i>disable</i>	Disable SSO.										
	<i>static</i>	Static SSO.										
<i>auto</i>	Auto SSO.											
sso-credential	Single sign-on credentials.	option	-	sslvpn-login								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sslvpn-login</i>	Agentless VPN login.		
	<i>alternative</i>	Alternative.		
sso-password	SSO password.	password	Not Specified	
sso-username	SSO user name.	var-string	Maximum length: 35	
url	Landing page URL.	var-string	Maximum length: 511	

config form-data

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

config vpn ssl web realm



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Realm.

```
config vpn ssl web realm
  Description: Realm.
  edit <url-path>
    set login-page {var-string}
    set max-concurrent-user {integer}
    set nas-ip {ipv4-address}
    set radius-port {integer}
    set radius-server {string}
    set virtual-host {var-string}
    set virtual-host-only [enable|disable]
    set virtual-host-server-cert {string}
  next
end
```

config vpn ssl web realm

Parameter	Description	Type	Size	Default						
login-page	Replacement HTML for Agentless VPN login page.	var-string	Maximum length: 32768							
max-concurrent-user	Maximum concurrent users (0 - 65535, 0 means unlimited).	integer	Minimum value: 0 Maximum value: 65535	0						
nas-ip	IP address used as a NAS-IP to communicate with the RADIUS server.	ipv4-address	Not Specified	0.0.0.0						
radius-port	RADIUS service port number (0 - 65535, 0 means user.radius.radius-port).	integer	Minimum value: 0 Maximum value: 65535	0						
radius-server	RADIUS server associated with realm.	string	Maximum length: 35							
url-path	URL path to access Agentless VPN login page.	string	Maximum length: 35							
virtual-host	Virtual host name for realm.	var-string	Maximum length: 255							
virtual-host-only	Enable/disable enforcement of virtual host method for Agentless VPN client access.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
virtual-host-server-cert	Name of the server certificate to used for this realm.	string	Maximum length: 35							

config vpn ssl web user-bookmark



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure Agentless VPN user bookmark.

```
config vpn ssl web user-bookmark
  Description: Configure Agentless VPN user bookmark.
  edit <name>
    config bookmarks
      Description: Bookmark table.
      edit <name>
        set additional-params {var-string}
        set apptype [ftp|rdp|...]
        set color-depth [32|16|...]
        set description {var-string}
        set domain {var-string}
        set folder {var-string}
        config form-data
          Description: Form data.
          edit <name>
            set value {var-string}
          next
        end
        set height {integer}
        set host {var-string}
        set keyboard-layout [ar-101|ar-102|...]
        set load-balancing-info {var-string}
```



```

        set logon-password {password}
        set logon-user {var-string}
        set port {integer}
        set preconnection-blob {var-string}
        set preconnection-id {integer}
        set restricted-admin [enable|disable]
        set security [any|rdp|...]
        set send-preconnection-id [enable|disable]
        set sso [disable|static|...]
        set sso-credential [sslvpn-login|alternative]
        set sso-credential-sent-once [enable|disable]
        set sso-password {password}
        set sso-username {var-string}
        set url {var-string}
        set vnc-keyboard-layout [default|da|...]
        set width {integer}
    next
end
    set custom-lang {string}
next
end

```

config vpn ssl web user-bookmark

Parameter	Description	Type	Size	Default
custom-lang	Personal language.	string	Maximum length: 35	
name	User and group name.	string	Maximum length: 101	

config bookmarks

Parameter	Description	Type	Size	Default
additional-params	Additional parameters.	var-string	Maximum length: 128	
apptype	Application type.	option	-	web
	Option		Description	
	ftp		FTP.	
	rdp		RDP.	
	sftp		SFTP.	
	smb		SMB/CIFS.	

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssh</td><td>SSH.</td></tr><tr><td>telnet</td><td>Telnet.</td></tr><tr><td>vnc</td><td>VNC.</td></tr><tr><td>web</td><td>HTTP/HTTPS.</td></tr></table>	Option	Description	ssh	SSH.	telnet	Telnet.	vnc	VNC.	web	HTTP/HTTPS.											
	Option	Description																				
	ssh	SSH.																				
	telnet	Telnet.																				
	vnc	VNC.																				
web	HTTP/HTTPS.																					
color-depth	Color depth per pixel.	option	-	16																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>32</td><td>32bits per pixel.</td></tr><tr><td>16</td><td>16bits per pixel.</td></tr><tr><td>8</td><td>8bits per pixel.</td></tr></table>	Option	Description	32	32bits per pixel.	16	16bits per pixel.	8	8bits per pixel.													
	Option	Description																				
	32	32bits per pixel.																				
	16	16bits per pixel.																				
8	8bits per pixel.																					
description	Description.	var-string	Maximum length: 128																			
domain	Login domain.	var-string	Maximum length: 128																			
folder	Network shared file folder parameter.	var-string	Maximum length: 128																			
height	Screen height (range from 0 - 65535, default = 0).	integer	Minimum value: 0 0 Maximum value: 65535																			
host	Host name/IP parameter.	var-string	Maximum length: 128																			
keyboard-layout	Keyboard layout.	option	-	en-us																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ar-101</td><td>Arabic (101).</td></tr><tr><td>ar-102</td><td>Arabic (102).</td></tr><tr><td>ar-102-azerty</td><td>Arabic (102) AZERTY.</td></tr><tr><td>can-mul</td><td>Canadian Multilingual Standard.</td></tr><tr><td>cz</td><td>Czech.</td></tr><tr><td>cz-qwerty</td><td>Czech (QWERTY).</td></tr><tr><td>cz-pr</td><td>Czech Programmers.</td></tr><tr><td>da</td><td>Danish.</td></tr></table>	Option	Description	ar-101	Arabic (101).	ar-102	Arabic (102).	ar-102-azerty	Arabic (102) AZERTY.	can-mul	Canadian Multilingual Standard.	cz	Czech.	cz-qwerty	Czech (QWERTY).	cz-pr	Czech Programmers.	da	Danish.			
	Option	Description																				
	ar-101	Arabic (101).																				
	ar-102	Arabic (102).																				
	ar-102-azerty	Arabic (102) AZERTY.																				
	can-mul	Canadian Multilingual Standard.																				
	cz	Czech.																				
	cz-qwerty	Czech (QWERTY).																				
	cz-pr	Czech Programmers.																				
da	Danish.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>nl</i>	Dutch.		
	<i>de</i>	German.		
	<i>de-ch</i>	German, Switzerland.		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finnish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-apple</i>	French, Apple.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgium.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ja-106</i>	Japanese 106/109 key.		
	<i>ko</i>	Korean.		
	<i>la-am</i>	Latin American.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		
	<i>lt-std</i>	Lithuanian Standard.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>lav-std</i>	Latvian (Standard).			
	<i>lav-leg</i>	Latvian (Legacy).			
	<i>mk</i>	Macedonian (FYROM).			
	<i>mk-std</i>	Macedonia (FYROM) - Standard.			
	<i>no</i>	Norwegian.			
	<i>no-sami</i>	Norwegian with Sami.			
	<i>pol-214</i>	Polish (214).			
	<i>pol-pr</i>	Polish (Programmers).			
	<i>pt</i>	Portuguese.			
	<i>pt-br</i>	Portuguese (Brazilian ABNT).			
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).			
	<i>ru</i>	Russian.			
	<i>ru-mne</i>	Russian - Mnemonic.			
	<i>ru-t</i>	Russian (Typewriter).			
	<i>sl</i>	Slovenian.			
	<i>sv</i>	Swedish.			
	<i>sv-sami</i>	Swedish with Sami.			
	<i>tuk</i>	Turkmen.			
	<i>tur-f</i>	Turkish F.			
	<i>tur-q</i>	Turkish Q.			
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.			
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.			
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).			
	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.			
	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.			
	load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511	
	logon-password	Logon password.	password	Not Specified	

Parameter	Description	Type	Size	Default										
logon-user	Logon user.	var-string	Maximum length: 35											
name	Bookmark name.	string	Maximum length: 35											
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535											
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511											
preconnection-id	The numeric ID of the RDP source (0-4294967295).	integer	Minimum value: 0 Maximum value: 4294967295											
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable restricted admin mode for RDP.</td></tr><tr><td><i>disable</i></td><td>Disable restricted admin mode for RDP.</td></tr></table>				Option	Description	<i>enable</i>	Enable restricted admin mode for RDP.	<i>disable</i>	Disable restricted admin mode for RDP.				
Option	Description													
<i>enable</i>	Enable restricted admin mode for RDP.													
<i>disable</i>	Disable restricted admin mode for RDP.													
security	Security mode for RDP connection (default = any).	option	-	any										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Allow the server to choose the type of security.</td></tr><tr><td><i>rdp</i></td><td>Standard RDP encryption.</td></tr><tr><td><i>nla</i></td><td>Network Level Authentication.</td></tr><tr><td><i>tls</i></td><td>TLS encryption.</td></tr></table>				Option	Description	<i>any</i>	Allow the server to choose the type of security.	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.
Option	Description													
<i>any</i>	Allow the server to choose the type of security.													
<i>rdp</i>	Standard RDP encryption.													
<i>nla</i>	Network Level Authentication.													
<i>tls</i>	TLS encryption.													
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of preconnection ID.</td></tr><tr><td><i>disable</i></td><td>Disable sending of preconnection ID.</td></tr></table>				Option	Description	<i>enable</i>	Enable sending of preconnection ID.	<i>disable</i>	Disable sending of preconnection ID.				
Option	Description													
<i>enable</i>	Enable sending of preconnection ID.													
<i>disable</i>	Disable sending of preconnection ID.													
sso	Single sign-on.	option	-	disable										

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSO.</td></tr><tr><td><i>static</i></td><td>Static SSO.</td></tr><tr><td><i>auto</i></td><td>Auto SSO.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSO.	<i>static</i>	Static SSO.	<i>auto</i>	Auto SSO.											
	Option	Description																		
	<i>disable</i>	Disable SSO.																		
	<i>static</i>	Static SSO.																		
<i>auto</i>	Auto SSO.																			
sso-credential	Single sign-on credentials.	option	-	sslvpn-login																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sslvpn-login</i></td><td>Agentless VPN login.</td></tr><tr><td><i>alternative</i></td><td>Alternative.</td></tr></table>	Option	Description	<i>sslvpn-login</i>	Agentless VPN login.	<i>alternative</i>	Alternative.													
	Option	Description																		
	<i>sslvpn-login</i>	Agentless VPN login.																		
<i>alternative</i>	Alternative.																			
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Single sign-on credentials are only sent once to remote server.</td></tr><tr><td><i>disable</i></td><td>Single sign-on credentials are sent to remote server for every HTTP request.</td></tr></table>	Option	Description	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.													
	Option	Description																		
	<i>enable</i>	Single sign-on credentials are only sent once to remote server.																		
<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.																			
sso-password	SSO password.	password	Not Specified																	
sso-username	SSO user name.	var-string	Maximum length: 35																	
url	URL parameter.	var-string	Maximum length: 128																	
vnc-keyboard-layout	Keyboard layout.	option	-	default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Default.</td></tr><tr><td><i>da</i></td><td>Danish.</td></tr><tr><td><i>nl</i></td><td>Dutch.</td></tr><tr><td><i>en-uk</i></td><td>English, United Kingdom.</td></tr><tr><td><i>en-uk-ext</i></td><td>English, United Kingdom Extended.</td></tr><tr><td><i>fi</i></td><td>Finnish.</td></tr><tr><td><i>fr</i></td><td>French.</td></tr></table>	Option	Description	<i>default</i>	Default.	<i>da</i>	Danish.	<i>nl</i>	Dutch.	<i>en-uk</i>	English, United Kingdom.	<i>en-uk-ext</i>	English, United Kingdom Extended.	<i>fi</i>	Finnish.	<i>fr</i>	French.			
	Option	Description																		
	<i>default</i>	Default.																		
	<i>da</i>	Danish.																		
	<i>nl</i>	Dutch.																		
	<i>en-uk</i>	English, United Kingdom.																		
	<i>en-uk-ext</i>	English, United Kingdom Extended.																		
	<i>fi</i>	Finnish.																		
<i>fr</i>	French.																			

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fr-be</i></td><td>French, Belgium.</td></tr><tr><td><i>fr-ca-mul</i></td><td>French, Canadian Multilingual Std.</td></tr><tr><td><i>de</i></td><td>German.</td></tr><tr><td><i>de-ch</i></td><td>German, Switzerland.</td></tr><tr><td><i>it</i></td><td>Italian.</td></tr><tr><td><i>it-142</i></td><td>Italian (142).</td></tr><tr><td><i>pt</i></td><td>Portuguese.</td></tr><tr><td><i>pt-br-abnt2</i></td><td>Portuguese (Brazilian ABNT2).</td></tr><tr><td><i>no</i></td><td>Norwegian.</td></tr><tr><td><i>gd</i></td><td>Scottish Gaelic.</td></tr><tr><td><i>es</i></td><td>Spanish.</td></tr><tr><td><i>sv</i></td><td>Swedish.</td></tr><tr><td><i>us-intl</i></td><td>United States-International.</td></tr></table>	Option	Description	<i>fr-be</i>	French, Belgium.	<i>fr-ca-mul</i>	French, Canadian Multilingual Std.	<i>de</i>	German.	<i>de-ch</i>	German, Switzerland.	<i>it</i>	Italian.	<i>it-142</i>	Italian (142).	<i>pt</i>	Portuguese.	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).	<i>no</i>	Norwegian.	<i>gd</i>	Scottish Gaelic.	<i>es</i>	Spanish.	<i>sv</i>	Swedish.	<i>us-intl</i>	United States-International.			
	Option	Description																														
	<i>fr-be</i>	French, Belgium.																														
	<i>fr-ca-mul</i>	French, Canadian Multilingual Std.																														
	<i>de</i>	German.																														
	<i>de-ch</i>	German, Switzerland.																														
	<i>it</i>	Italian.																														
	<i>it-142</i>	Italian (142).																														
	<i>pt</i>	Portuguese.																														
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).																														
	<i>no</i>	Norwegian.																														
	<i>gd</i>	Scottish Gaelic.																														
	<i>es</i>	Spanish.																														
	<i>sv</i>	Swedish.																														
<i>us-intl</i>	United States-International.																															
width	Screen width (range from 0 - 65535, default = 0).	integer	Minimum value: 0 0 Maximum value: 65535																													

config form-data

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

config vpn ssl web user-group-bookmark



This command is available for model(s): FortiGate 1000D, FortiGate 1000F, FortiGate 1001F, FortiGate 100F, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 120G, FortiGate 121G, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3200F, FortiGate 3201F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3700F, FortiGate 3701F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 900G, FortiGate 901G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 90G, FortiGate 91G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F.

Configure Agentless VPN user group bookmark.

```
config vpn ssl web user-group-bookmark
  Description: Configure Agentless VPN user group bookmark.
  edit <name>
    config bookmarks
      Description: Bookmark table.
      edit <name>
        set additional-params {var-string}
        set apptype [ftp|rdp|...]
        set color-depth [32|16|...]
        set description {var-string}
        set domain {var-string}
        set folder {var-string}
        config form-data
          Description: Form data.
          edit <name>
            set value {var-string}
          next
        end
      end
    set height {integer}
    set host {var-string}
    set keyboard-layout [ar-101|ar-102|...]
    set load-balancing-info {var-string}
```



```

        set logon-password {password}
        set logon-user {var-string}
        set port {integer}
        set preconnection-blob {var-string}
        set preconnection-id {integer}
        set restricted-admin [enable|disable]
        set security [any|rdp|...]
        set send-preconnection-id [enable|disable]
        set sso [disable|static|...]
        set sso-credential [sslvpn-login|alternative]
        set sso-credential-sent-once [enable|disable]
        set sso-password {password}
        set sso-username {var-string}
        set url {var-string}
        set vnc-keyboard-layout [default|da|...]
        set width {integer}
    next
end
next
end

```

config vpn ssl web user-group-bookmark

Parameter	Description	Type	Size	Default
name	Group name.	string	Maximum length: 64	

config bookmarks

Parameter	Description	Type	Size	Default
additional-params	Additional parameters.	var-string	Maximum length: 128	
apptype	Application type.	option	-	web
	Option		Description	
	ftp	FTP.		
	rdp	RDP.		
	sftp	SFTP.		
	smb	SMB/CIFS.		
	ssh	SSH.		
	telnet	Telnet.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vnc</i></td><td>VNC.</td></tr><tr><td><i>web</i></td><td>HTTP/HTTPS.</td></tr></table>	Option	Description	<i>vnc</i>	VNC.	<i>web</i>	HTTP/HTTPS.																			
	Option	Description																								
	<i>vnc</i>	VNC.																								
<i>web</i>	HTTP/HTTPS.																									
color-depth	Color depth per pixel.	option	-	16																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>32</td><td>32bits per pixel.</td></tr><tr><td>16</td><td>16bits per pixel.</td></tr><tr><td>8</td><td>8bits per pixel.</td></tr></table>	Option	Description	32	32bits per pixel.	16	16bits per pixel.	8	8bits per pixel.																	
	Option	Description																								
	32	32bits per pixel.																								
	16	16bits per pixel.																								
8	8bits per pixel.																									
description	Description.	var-string	Maximum length: 128																							
domain	Login domain.	var-string	Maximum length: 128																							
folder	Network shared file folder parameter.	var-string	Maximum length: 128																							
height	Screen height (range from 0 - 65535, default = 0).	integer	Minimum value: 0 0 Maximum value: 65535																							
host	Host name/IP parameter.	var-string	Maximum length: 128																							
keyboard-layout	Keyboard layout.	option	-	en-us																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ar-101</i></td><td>Arabic (101).</td></tr><tr><td><i>ar-102</i></td><td>Arabic (102).</td></tr><tr><td><i>ar-102-azerty</i></td><td>Arabic (102) AZERTY.</td></tr><tr><td><i>can-mul</i></td><td>Canadian Multilingual Standard.</td></tr><tr><td><i>cz</i></td><td>Czech.</td></tr><tr><td><i>cz-qwerty</i></td><td>Czech (QWERTY).</td></tr><tr><td><i>cz-pr</i></td><td>Czech Programmers.</td></tr><tr><td><i>da</i></td><td>Danish.</td></tr><tr><td><i>nl</i></td><td>Dutch.</td></tr><tr><td><i>de</i></td><td>German.</td></tr></table>	Option	Description	<i>ar-101</i>	Arabic (101).	<i>ar-102</i>	Arabic (102).	<i>ar-102-azerty</i>	Arabic (102) AZERTY.	<i>can-mul</i>	Canadian Multilingual Standard.	<i>cz</i>	Czech.	<i>cz-qwerty</i>	Czech (QWERTY).	<i>cz-pr</i>	Czech Programmers.	<i>da</i>	Danish.	<i>nl</i>	Dutch.	<i>de</i>	German.			
	Option	Description																								
	<i>ar-101</i>	Arabic (101).																								
	<i>ar-102</i>	Arabic (102).																								
	<i>ar-102-azerty</i>	Arabic (102) AZERTY.																								
	<i>can-mul</i>	Canadian Multilingual Standard.																								
	<i>cz</i>	Czech.																								
	<i>cz-qwerty</i>	Czech (QWERTY).																								
	<i>cz-pr</i>	Czech Programmers.																								
	<i>da</i>	Danish.																								
	<i>nl</i>	Dutch.																								
<i>de</i>	German.																									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>de-ch</i>	German, Switzerland.		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finnish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-apple</i>	French, Apple.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgium.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ja-106</i>	Japanese 106/109 key.		
	<i>ko</i>	Korean.		
	<i>la-am</i>	Latin American.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		
	<i>lt-std</i>	Lithuanian Standard.		
	<i>lav-std</i>	Latvian (Standard).		
	<i>lav-leg</i>	Latvian (Legacy).		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mk</i>	Macedonian (FYROM).		
	<i>mk-std</i>	Macedonia (FYROM) - Standard.		
	<i>no</i>	Norwegian.		
	<i>no-sami</i>	Norwegian with Sami.		
	<i>pol-214</i>	Polish (214).		
	<i>pol-pr</i>	Polish (Programmers).		
	<i>pt</i>	Portuguese.		
	<i>pt-br</i>	Portuguese (Brazilian ABNT).		
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).		
	<i>ru</i>	Russian.		
	<i>ru-mne</i>	Russian - Mnemonic.		
	<i>ru-t</i>	Russian (Typewriter).		
	<i>sl</i>	Slovenian.		
	<i>sv</i>	Swedish.		
	<i>sv-sami</i>	Swedish with Sami.		
	<i>tuk</i>	Turkmen.		
	<i>tur-f</i>	Turkish F.		
	<i>tur-q</i>	Turkish Q.		
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.		
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.		
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).		
	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.		
	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.		
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511	
logon-password	Logon password.	password	Not Specified	
logon-user	Logon user.	var-string	Maximum length: 35	

Parameter	Description	Type	Size	Default										
name	Bookmark name.	string	Maximum length: 35											
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0										
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511											
preconnection-id	The numeric ID of the RDP source (0-4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0										
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable restricted admin mode for RDP.</td></tr><tr><td><i>disable</i></td><td>Disable restricted admin mode for RDP.</td></tr></table>	Option	Description	<i>enable</i>	Enable restricted admin mode for RDP.	<i>disable</i>	Disable restricted admin mode for RDP.							
Option	Description													
<i>enable</i>	Enable restricted admin mode for RDP.													
<i>disable</i>	Disable restricted admin mode for RDP.													
security	Security mode for RDP connection (default = any).	option	-	any										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Allow the server to choose the type of security.</td></tr><tr><td><i>rdp</i></td><td>Standard RDP encryption.</td></tr><tr><td><i>nla</i></td><td>Network Level Authentication.</td></tr><tr><td><i>tls</i></td><td>TLS encryption.</td></tr></table>	Option	Description	<i>any</i>	Allow the server to choose the type of security.	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.			
Option	Description													
<i>any</i>	Allow the server to choose the type of security.													
<i>rdp</i>	Standard RDP encryption.													
<i>nla</i>	Network Level Authentication.													
<i>tls</i>	TLS encryption.													
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of preconnection ID.</td></tr><tr><td><i>disable</i></td><td>Disable sending of preconnection ID.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of preconnection ID.	<i>disable</i>	Disable sending of preconnection ID.							
Option	Description													
<i>enable</i>	Enable sending of preconnection ID.													
<i>disable</i>	Disable sending of preconnection ID.													
sso	Single sign-on.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSO.</td></tr><tr><td><i>static</i></td><td>Static SSO.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSO.	<i>static</i>	Static SSO.							
Option	Description													
<i>disable</i>	Disable SSO.													
<i>static</i>	Static SSO.													

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Auto SSO.</td></tr></table>	Option	Description	<i>auto</i>	Auto SSO.																			
	Option	Description																						
<i>auto</i>	Auto SSO.																							
sso-credential	Single sign-on credentials.	option	-	sslvpn-login																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sslvpn-login</i></td><td>Agentless VPN login.</td></tr><tr><td><i>alternative</i></td><td>Alternative.</td></tr></table>	Option	Description	<i>sslvpn-login</i>	Agentless VPN login.	<i>alternative</i>	Alternative.																	
	Option	Description																						
	<i>sslvpn-login</i>	Agentless VPN login.																						
<i>alternative</i>	Alternative.																							
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Single sign-on credentials are only sent once to remote server.</td></tr><tr><td><i>disable</i></td><td>Single sign-on credentials are sent to remote server for every HTTP request.</td></tr></table>	Option	Description	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.																	
	Option	Description																						
	<i>enable</i>	Single sign-on credentials are only sent once to remote server.																						
<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.																							
sso-password	SSO password.	password	Not Specified																					
sso-username	SSO user name.	var-string	Maximum length: 35																					
url	URL parameter.	var-string	Maximum length: 128																					
vnc-keyboard-layout	Keyboard layout.	option	-	default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Default.</td></tr><tr><td><i>da</i></td><td>Danish.</td></tr><tr><td><i>nl</i></td><td>Dutch.</td></tr><tr><td><i>en-uk</i></td><td>English, United Kingdom.</td></tr><tr><td><i>en-uk-ext</i></td><td>English, United Kingdom Extended.</td></tr><tr><td><i>fi</i></td><td>Finnish.</td></tr><tr><td><i>fr</i></td><td>French.</td></tr><tr><td><i>fr-be</i></td><td>French, Belgium.</td></tr><tr><td><i>fr-ca-mul</i></td><td>French, Canadian Multilingual Std.</td></tr></table>	Option	Description	<i>default</i>	Default.	<i>da</i>	Danish.	<i>nl</i>	Dutch.	<i>en-uk</i>	English, United Kingdom.	<i>en-uk-ext</i>	English, United Kingdom Extended.	<i>fi</i>	Finnish.	<i>fr</i>	French.	<i>fr-be</i>	French, Belgium.	<i>fr-ca-mul</i>	French, Canadian Multilingual Std.			
	Option	Description																						
	<i>default</i>	Default.																						
	<i>da</i>	Danish.																						
	<i>nl</i>	Dutch.																						
	<i>en-uk</i>	English, United Kingdom.																						
	<i>en-uk-ext</i>	English, United Kingdom Extended.																						
	<i>fi</i>	Finnish.																						
	<i>fr</i>	French.																						
	<i>fr-be</i>	French, Belgium.																						
<i>fr-ca-mul</i>	French, Canadian Multilingual Std.																							

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>de</i></td><td>German.</td></tr><tr><td><i>de-ch</i></td><td>German, Switzerland.</td></tr><tr><td><i>it</i></td><td>Italian.</td></tr><tr><td><i>it-142</i></td><td>Italian (142).</td></tr><tr><td><i>pt</i></td><td>Portuguese.</td></tr><tr><td><i>pt-br-abnt2</i></td><td>Portuguese (Brazilian ABNT2).</td></tr><tr><td><i>no</i></td><td>Norwegian.</td></tr><tr><td><i>gd</i></td><td>Scottish Gaelic.</td></tr><tr><td><i>es</i></td><td>Spanish.</td></tr><tr><td><i>sv</i></td><td>Swedish.</td></tr><tr><td><i>us-intl</i></td><td>United States-International.</td></tr></table>	Option	Description	<i>de</i>	German.	<i>de-ch</i>	German, Switzerland.	<i>it</i>	Italian.	<i>it-142</i>	Italian (142).	<i>pt</i>	Portuguese.	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).	<i>no</i>	Norwegian.	<i>gd</i>	Scottish Gaelic.	<i>es</i>	Spanish.	<i>sv</i>	Swedish.	<i>us-intl</i>	United States-International.			
	Option	Description																										
	<i>de</i>	German.																										
	<i>de-ch</i>	German, Switzerland.																										
	<i>it</i>	Italian.																										
	<i>it-142</i>	Italian (142).																										
	<i>pt</i>	Portuguese.																										
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).																										
	<i>no</i>	Norwegian.																										
	<i>gd</i>	Scottish Gaelic.																										
	<i>es</i>	Spanish.																										
	<i>sv</i>	Swedish.																										
<i>us-intl</i>	United States-International.																											
width	Screen width (range from 0 - 65535, default = 0).	integer	Minimum value: 0 0 Maximum value: 65535																									

config form-data

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

waf

This section includes syntax for the following commands:

- [config waf main-class on page 2296](#)
- [config waf profile on page 2296](#)
- [config waf signature on page 2321](#)
- [config waf sub-class on page 2321](#)

config waf main-class

Hidden table for datasource.

```
config waf main-class
  Description: Hidden table for datasource.
  edit <id>
    set name {string}
  next
end
```

config waf main-class

Parameter	Description	Type	Size	Default
id	Main signature class ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
name	Main signature class name.	string	Maximum length: 127	

config waf profile

Configure Web application firewall configuration.

```
config waf profile
  Description: Configure Web application firewall configuration.
  edit <name>
    config address-list
      Description: Address block and allow lists.
      set blocked-address <name1>, <name2>, ...
```



```

    set blocked-log [enable|disable]
    set severity [high|medium|...]
    set status [enable|disable]
    set trusted-address <name1>, <name2>, ...
end
set comment {var-string}
config constraint
    Description: WAF HTTP protocol restrictions.
    config content-length
        Description: HTTP content length in request.
        set action [allow|block]
        set length {integer}
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config exception
        Description: HTTP constraint exception.
        edit <id>
            set address {string}
            set content-length [enable|disable]
            set header-length [enable|disable]
            set hostname [enable|disable]
            set line-length [enable|disable]
            set malformed [enable|disable]
            set max-cookie [enable|disable]
            set max-header-line [enable|disable]
            set max-range-segment [enable|disable]
            set max-url-param [enable|disable]
            set method [enable|disable]
            set param-length [enable|disable]
            set pattern {string}
            set regex [enable|disable]
            set url-param-length [enable|disable]
            set version [enable|disable]
        next
    end
    config header-length
        Description: HTTP header length in request.
        set action [allow|block]
        set length {integer}
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config hostname
        Description: Enable/disable hostname check.
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
end

```

```

config line-length
    Description: HTTP line length in request.
    set action [allow|block]
    set length {integer}
    set log [enable|disable]
    set severity [high|medium|...]
    set status [enable|disable]
end
config malformed
    Description: Enable/disable malformed HTTP request check.
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]
    set status [enable|disable]
end
config max-cookie
    Description: Maximum number of cookies in HTTP request.
    set action [allow|block]
    set log [enable|disable]
    set max-cookie {integer}
    set severity [high|medium|...]
    set status [enable|disable]
end
config max-header-line
    Description: Maximum number of HTTP header line.
    set action [allow|block]
    set log [enable|disable]
    set max-header-line {integer}
    set severity [high|medium|...]
    set status [enable|disable]
end
config max-range-segment
    Description: Maximum number of range segments in HTTP range line.
    set action [allow|block]
    set log [enable|disable]
    set max-range-segment {integer}
    set severity [high|medium|...]
    set status [enable|disable]
end
config max-url-param
    Description: Maximum number of parameters in URL.
    set action [allow|block]
    set log [enable|disable]
    set max-url-param {integer}
    set severity [high|medium|...]
    set status [enable|disable]
end
config method
    Description: Enable/disable HTTP method check.
    set action [allow|block]
    set log [enable|disable]
    set severity [high|medium|...]

```

```

        set status [enable|disable]
    end
    config param-length
        Description: Maximum length of parameter in URL, HTTP POST request or HTTP body.
        set action [allow|block]
        set length {integer}
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config url-param-length
        Description: Maximum length of parameter in URL.
        set action [allow|block]
        set length {integer}
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config version
        Description: Enable/disable HTTP version check.
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
end
set extended-log [enable|disable]
set external [disable|enable]
config method
    Description: Method restriction.
    set default-allowed-methods {option1}, {option2}, ...
    set log [enable|disable]
    config method-policy
        Description: HTTP method policy.
        edit <id>
            set address {string}
            set allowed-methods {option1}, {option2}, ...
            set pattern {string}
            set regex [enable|disable]
        next
    end
    set severity [high|medium|...]
    set status [enable|disable]
end
config signature
    Description: WAF signatures.
    set credit-card-detection-threshold {integer}
    config custom-signature
        Description: Custom signature.
        edit <name>
            set action [allow|block|...]
            set case-sensitivity [disable|enable]
        end
    end
end

```

```

        set direction [request|response]
        set log [enable|disable]
        set pattern {string}
        set severity [high|medium|...]
        set status [enable|disable]
        set target {option1}, {option2}, ...
    next
end
set disabled-signature <id1>, <id2>, ...
set disabled-sub-class <id1>, <id2>, ...
config main-class
    Description: Main signature class. Read-only.
    edit <id>
        set action [allow|block|...]
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    next
end
end
config url-access
    Description: URL access list.
    edit <id>
        config access-pattern
            Description: URL access pattern.
            edit <id>
                set negate [enable|disable]
                set pattern {string}
                set regex [enable|disable]
                set srcaddr {string}
            next
        end
        set action [bypass|permit|...]
        set address {string}
        set log [enable|disable]
        set severity [high|medium|...]
    next
end
next
end
end

```

config waf profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
extended-log	Enable/disable extended logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
external	Disable/Enable external HTTP Inspection.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable external inspection.		
	<i>enable</i>	Enable external inspection.		
name	WAF Profile name.	string	Maximum length: 47	

config address-list

Parameter	Description	Type	Size	Default
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79	
blocked-log	Enable/disable logging on blocked addresses.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79	

config content-length

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
length	Length of HTTP content in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	67108864
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config exception

Parameter	Description	Type	Size	Default
address	Host address.	string	Maximum length: 79	
content-length	HTTP content length in request.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
header-length	HTTP header length in request.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
hostname	Enable/disable hostname check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
id	Exception ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
line-length	HTTP line length in request.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
malformed	Enable/disable malformed HTTP request check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-cookie	Maximum number of cookies in HTTP request.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
max-header-line	Maximum number of HTTP header line.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
max-range-segment	Maximum number of range segments in HTTP range line.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
max-url-param	Maximum number of parameters in URL.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
method	Enable/disable HTTP method check.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
param-length	Maximum length of parameter in URL, HTTP POST request or HTTP body.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
pattern	URL pattern.	string	Maximum length: 511							
regex	Enable/disable regular expression based pattern match.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
url-param-length	Maximum length of parameter in URL.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
version	Enable/disable HTTP version check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config header-length

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
length	Length of HTTP header in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config hostname

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config line-length

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	1024
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config malformed

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		

Parameter	Description	Type	Size	Default
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config max-cookie

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-cookie	Maximum number of cookies in HTTP request (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config max-header-line

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-header-line	Maximum number HTTP header lines (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	32
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config max-range-segment

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-range-segment	Maximum number of range segments in HTTP range line (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	5
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config max-url-param

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-url-param	Maximum number of parameters in URL (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config method

Parameter	Description	Type	Size	Default						
action	Action.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>block</i></td><td>Block.</td></tr></table>				Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.
	Option	Description								
	<i>allow</i>	Allow.								
<i>block</i>	Block.									

Parameter	Description	Type	Size	Default								
log	Enable/disable logging.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High severity.</td></tr><tr><td><i>medium</i></td><td>Medium severity.</td></tr><tr><td><i>low</i></td><td>Low severity.</td></tr></table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
Option	Description											
<i>high</i>	High severity.											
<i>medium</i>	Medium severity.											
<i>low</i>	Low severity.											
status	Enable/disable the constraint.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

config param-length

Parameter	Description	Type	Size	Default						
action	Action.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>block</i></td><td>Block.</td></tr></table>				Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.
	Option	Description								
	<i>allow</i>	Allow.								
<i>block</i>	Block.									
length	Maximum length of parameter in URL, HTTP POST request or HTTP body in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192						
log	Enable/disable logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
severity	Severity.	option	-	medium						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config url-param-length

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
length	Maximum length of URL parameter in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config version

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config method

Parameter	Description	Type	Size	Default
default-allowed-methods	Methods.	option	-	

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>get</td><td>HTTP GET method.</td></tr><tr><td>post</td><td>HTTP POST method.</td></tr><tr><td>put</td><td>HTTP PUT method.</td></tr><tr><td>head</td><td>HTTP HEAD method.</td></tr><tr><td>connect</td><td>HTTP CONNECT method.</td></tr><tr><td>trace</td><td>HTTP TRACE method.</td></tr><tr><td>options</td><td>HTTP OPTIONS method.</td></tr><tr><td>delete</td><td>HTTP DELETE method.</td></tr><tr><td>others</td><td>Other HTTP methods.</td></tr></table>	Option	Description	get	HTTP GET method.	post	HTTP POST method.	put	HTTP PUT method.	head	HTTP HEAD method.	connect	HTTP CONNECT method.	trace	HTTP TRACE method.	options	HTTP OPTIONS method.	delete	HTTP DELETE method.	others	Other HTTP methods.			
	Option	Description																						
	get	HTTP GET method.																						
	post	HTTP POST method.																						
	put	HTTP PUT method.																						
	head	HTTP HEAD method.																						
	connect	HTTP CONNECT method.																						
	trace	HTTP TRACE method.																						
	options	HTTP OPTIONS method.																						
	delete	HTTP DELETE method.																						
others	Other HTTP methods.																							
log	Enable/disable logging.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.																	
	Option	Description																						
	enable	Enable setting.																						
disable	Disable setting.																							
severity	Severity.	option	-	medium																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High severity</td></tr><tr><td>medium</td><td>medium severity</td></tr><tr><td>low</td><td>low severity</td></tr></table>	Option	Description	high	High severity	medium	medium severity	low	low severity															
	Option	Description																						
	high	High severity																						
	medium	medium severity																						
low	low severity																							
status	Status.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.																	
	Option	Description																						
	enable	Enable setting.																						
disable	Disable setting.																							

config method-policy

Parameter	Description	Type	Size	Default
address	Host address.	string	Maximum length: 79	
allowed-methods	Allowed Methods.	option	-	

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>get</i></td><td>HTTP GET method.</td></tr><tr><td><i>post</i></td><td>HTTP POST method.</td></tr><tr><td><i>put</i></td><td>HTTP PUT method.</td></tr><tr><td><i>head</i></td><td>HTTP HEAD method.</td></tr><tr><td><i>connect</i></td><td>HTTP CONNECT method.</td></tr><tr><td><i>trace</i></td><td>HTTP TRACE method.</td></tr><tr><td><i>options</i></td><td>HTTP OPTIONS method.</td></tr><tr><td><i>delete</i></td><td>HTTP DELETE method.</td></tr><tr><td><i>others</i></td><td>Other HTTP methods.</td></tr></table>	Option	Description	<i>get</i>	HTTP GET method.	<i>post</i>	HTTP POST method.	<i>put</i>	HTTP PUT method.	<i>head</i>	HTTP HEAD method.	<i>connect</i>	HTTP CONNECT method.	<i>trace</i>	HTTP TRACE method.	<i>options</i>	HTTP OPTIONS method.	<i>delete</i>	HTTP DELETE method.	<i>others</i>	Other HTTP methods.			
	Option	Description																						
	<i>get</i>	HTTP GET method.																						
	<i>post</i>	HTTP POST method.																						
	<i>put</i>	HTTP PUT method.																						
	<i>head</i>	HTTP HEAD method.																						
	<i>connect</i>	HTTP CONNECT method.																						
	<i>trace</i>	HTTP TRACE method.																						
	<i>options</i>	HTTP OPTIONS method.																						
	<i>delete</i>	HTTP DELETE method.																						
<i>others</i>	Other HTTP methods.																							
id	HTTP method policy ID.	integer	Minimum value: 0 0 Maximum value: 4294967295																					
pattern	URL pattern.	string	Maximum length: 511																					
regex	Enable/disable regular expression based pattern match.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																	
	Option	Description																						
	<i>enable</i>	Enable setting.																						
<i>disable</i>	Disable setting.																							

config signature

Parameter	Description	Type	Size	Default
credit-card-detection-threshold	The minimum number of Credit cards to detect violation.	integer	Minimum value: 0 0 Maximum value: 128	3
disabled-signature <id>	Disabled signatures. Signature ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
disabled-sub-class <id>	Disabled signature subclasses. Signature subclass ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

config custom-signature

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
	<i>erase</i>	Erase credit card numbers.		
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	Option	Description		
	<i>disable</i>	Case insensitive in pattern.		
	<i>enable</i>	Case sensitive in pattern.		
direction	Traffic direction.	option	-	request
	Option	Description		
	<i>request</i>	Match HTTP request.		
	<i>response</i>	Match HTTP response.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
name	Signature name.	string	Maximum length: 35	
pattern	Match pattern.	string	Maximum length: 511	
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
status	Status.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
target	Match HTTP target.	option	-	
	Option	Description		
	<i>arg</i>	HTTP arguments.		
	<i>arg-name</i>	Names of HTTP arguments.		
	<i>req-body</i>	HTTP request body.		
	<i>req-cookie</i>	HTTP request cookies.		
	<i>req-cookie-name</i>	HTTP request cookie names.		
	<i>req-filename</i>	HTTP request file name.		
	<i>req-header</i>	HTTP request headers.		
	<i>req-header-name</i>	HTTP request header names.		
	<i>req-raw-uri</i>	Raw URI of HTTP request.		
	<i>req-uri</i>	URI of HTTP request.		
	<i>resp-body</i>	HTTP response body.		
	<i>resp-hdr</i>	HTTP response headers.		
	<i>resp-status</i>	HTTP response status.		

config main-class

Parameter	Description	Type	Size	Default
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
	<i>erase</i>	Erase credit card numbers.		

Parameter	Description	Type	Size	Default								
id	Main signature class ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0								
log	Enable/disable logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.		
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
severity	Severity.	option	-	medium								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High severity.</td></tr><tr><td>medium</td><td>Medium severity.</td></tr><tr><td>low</td><td>Low severity.</td></tr></table>				Option	Description	high	High severity.	medium	Medium severity.	low	Low severity.
	Option	Description										
	high	High severity.										
	medium	Medium severity.										
low	Low severity.											
status	Status.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.		
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											

config url-access

Parameter	Description	Type	Size	Default
action	Action.	option	-	permit
	Option	Description		
	bypass	Allow the HTTP request, also bypass further WAF scanning.		
	permit	Allow the HTTP request, and continue further WAF scanning.		
	block	Block HTTP request.		
address	Host address.	string	Maximum length: 79	
id	URL access ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config access-pattern

Parameter	Description	Type	Size	Default
id	URL access pattern ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
negate	Enable/disable match negation.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
srcaddr	Source address.	string	Maximum length: 79	

config waf signature

Hidden table for datasource.

```
config waf signature
  Description: Hidden table for datasource.
  edit <id>
    set desc {string}
  next
end
```

config waf signature

Parameter	Description	Type	Size	Default
desc	Signature description.	string	Maximum length: 511	
id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config waf sub-class

Hidden table for datasource.

```
config waf sub-class
  Description: Hidden table for datasource.
  edit <id>
    set name {string}
  next
end
```

config waf sub-class

Parameter	Description	Type	Size	Default
id	Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Signature subclass name.	string	Maximum length: 127	

wanopt

This section includes syntax for the following commands:

- [config wanopt auth-group on page 2322](#)
- [config wanopt cache-service on page 2324](#)
- [config wanopt content-delivery-network-rule on page 2327](#)
- [config wanopt peer on page 2333](#)
- [config wanopt profile on page 2334](#)
- [config wanopt remote-storage on page 2343](#)
- [config wanopt settings on page 2344](#)
- [config wanopt webcache on page 2346](#)

config wanopt auth-group



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R.

Configure WAN optimization authentication groups.

```

config wanopt auth-group
  Description: Configure WAN optimization authentication groups.
  edit <name>
    set auth-method [cert|psk]
    set cert {string}
    set peer {string}
    set peer-accept [any|defined|...]
    set psk {password}
  next
end

```

config wanopt auth-group

Parameter	Description	Type	Size	Default
auth-method	Select certificate or pre-shared key authentication for this authentication group.	option	-	cert
	Option	Description		
	<i>cert</i>	Certificate authentication.		
	<i>psk</i>	Pre-shared secret key authentication.		
cert	Name of certificate to identify this peer.	string	Maximum length: 35	
name	Auth-group name.	string	Maximum length: 35	
peer	If peer-accept is set to one, select the name of one peer to add to this authentication group. The peer must have added with the wanopt peer command.	string	Maximum length: 35	
peer-accept	Determine if this auth group accepts, any peer, a list of defined peers, or just one peer.	option	-	any
	Option	Description		
	<i>any</i>	Accept any peer that can authenticate with this auth group.		
	<i>defined</i>	Accept only the peers added with the wanopt peer command.		
	<i>one</i>	Accept the peer added to this auth group using the peer option.		
psk	Pre-shared key used by the peers in this authentication group.	password	Not Specified	

config wanopt cache-service



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R.

Designate cache-service for wan-optimization and webcache.

```
config wanopt cache-service
  Description: Designate cache-service for wan-optimization and webcache.
  set acceptable-connections [any|peers]
  set collaboration [enable|disable]
  set device-id {string}
  config dst-peer
    Description: Modify cache-service destination peer list.
    edit <device-id>
      set auth-type {integer}
      set encode-type {integer}
      set ip {ipv4-address-any}
      set priority {integer}
    next
  end
  set prefer-scenario [balance|prefer-speed|...]
  config src-peer
    Description: Modify cache-service source peer list.
    edit <device-id>
      set auth-type {integer}
      set encode-type {integer}
      set ip {ipv4-address-any}
```

```

        set priority {integer}
    next
end
end

```

config wanopt cache-service

Parameter	Description	Type	Size	Default
acceptable-connections	Set strategy when accepting cache collaboration connection.	option	-	any
	Option	Description		
	<i>any</i>	We can accept any cache-collaboration connection.		
	<i>peers</i>	We can only accept connections that are already in src-peers.		
collaboration	Enable/disable cache-collaboration between cache-service clusters.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable cache cache-collaboration.		
	<i>disable</i>	Disable cache cache-collaboration.		
device-id	Set identifier for this cache device.	string	Maximum length: 35	default_dev_id
prefer-scenario	Set the preferred cache behavior towards the balance between latency and hit-ratio.	option	-	balance
	Option	Description		
	<i>balance</i>	Balance between speed and cache hit ratio.		
	<i>prefer-speed</i>	Prefer response speed at the expense of increased cache bypasses.		
	<i>prefer-cache</i>	Prefer improving hit-ratio through increasing latency tolerance.		

config dst-peer

Parameter	Description	Type	Size	Default
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
device-id	Device ID of this peer.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1

config src-peer

Parameter	Description	Type	Size	Default
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
device-id	Device ID of this peer.	string	Maximum length: 35	
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1

config wanopt content-delivery-network-rule



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R.

Configure WAN optimization content delivery network rules.

```
config wanopt content-delivery-network-rule
  Description: Configure WAN optimization content delivery network rules.
  edit <name>
    set category [vcache|youtube]
    set comment {var-string}
    set host-domain-name-suffix <name1>, <name2>, ...
    set request-cache-control [enable|disable]
    set response-cache-control [enable|disable]
    set response-expires [enable|disable]
  config rules
    Description: WAN optimization content delivery network rule entries.
    edit <name>
      config content-id
        Description: Content ID settings.
        set end-direction [forward|backward]
        set end-skip {integer}
        set end-str {string}
        set range-str {string}
        set start-direction [forward|backward]
        set start-skip {integer}
        set start-str {string}
```

```

        set target [path|parameter|...]
    end
    config match-entries
        Description: List of entries to match.
        edit <id>
            set pattern <string1>, <string2>, ...
            set target [path|parameter|...]
        next
    end
    set match-mode [all|any]
    config skip-entries
        Description: List of entries to skip.
        edit <id>
            set pattern <string1>, <string2>, ...
            set target [path|parameter|...]
        next
    end
    set skip-rule-mode [all|any]
next
end
set status [enable|disable]
set updateserver [enable|disable]
next
end

```

config wanopt content-delivery-network-rule

Parameter	Description	Type	Size	Default						
category	Content delivery network rule category.	option	-	vcache						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>vcache</td><td>Vcache content delivery network.</td></tr><tr><td>youtube</td><td>Youtube content delivery network.</td></tr></table>				Option	Description	vcache	Vcache content delivery network.	youtube	Youtube content delivery network.
	Option	Description								
	vcache	Vcache content delivery network.								
youtube	Youtube content delivery network.									
comment	Comment about this CDN-rule.	var-string	Maximum length: 255							
host-domain-name-suffix <name>	Suffix portion of the fully qualified domain name. For example, fortinet.com in "www.fortinet.com". Suffix portion of the fully qualified domain name.	string	Maximum length: 79							
name	Name of table.	string	Maximum length: 35							
request-cache-control	Enable/disable HTTP request cache control.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
response-cache-control	Enable/disable HTTP response cache control.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
response-expires	Enable/disable HTTP response cache expires.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
status	Enable/disable WAN optimization content delivery network rules.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
updateserver	Enable/disable update server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config rules

Parameter	Description	Type	Size	Default
match-mode	Match criteria for collecting content ID.	option	-	all
	Option	Description		
	<i>all</i>	Must match all of the match entries.		
	<i>any</i>	Must match any of the match entries.		

Parameter	Description	Type	Size	Default						
name	WAN optimization content delivery network rule name.	string	Maximum length: 35							
skip-rule-mode	Skip mode when evaluating skip-rules.	option	-	all						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Must match all skip entries.</td></tr><tr><td><i>any</i></td><td>Must match any skip entries.</td></tr></table>				Option	Description	<i>all</i>	Must match all skip entries.	<i>any</i>	Must match any skip entries.
Option	Description									
<i>all</i>	Must match all skip entries.									
<i>any</i>	Must match any skip entries.									

config content-id

Parameter	Description	Type	Size	Default						
end-direction	Search direction from end-str match.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward direction.</td></tr><tr><td><i>backward</i></td><td>Backward direction.</td></tr></table>				Option	Description	<i>forward</i>	Forward direction.	<i>backward</i>	Backward direction.
	Option	Description								
	<i>forward</i>	Forward direction.								
<i>backward</i>	Backward direction.									
end-skip	Number of characters in URL to skip after end-str has been matched.	integer	Minimum value: 0 0 Maximum value: 4294967295							
end-str	String from which to end search.	string	Maximum length: 35							
range-str	Name of content ID within the start string and end string.	string	Maximum length: 35							
start-direction	Search direction from start-str match.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward direction.</td></tr><tr><td><i>backward</i></td><td>Backward direction.</td></tr></table>				Option	Description	<i>forward</i>	Forward direction.	<i>backward</i>	Backward direction.
	Option	Description								
	<i>forward</i>	Forward direction.								
<i>backward</i>	Backward direction.									
start-skip	Number of characters in URL to skip after start-str has been matched.	integer	Minimum value: 0 0 Maximum value: 4294967295							
start-str	String from which to start search.	string	Maximum length: 35	/						

Parameter	Description	Type	Size	Default
target	Option in HTTP header or URL parameter to match.	option	-	path
	Option	Description		
	<i>path</i>	Match with the URL path.		
	<i>parameter</i>	Match with the URL parameters.		
	<i>referrer</i>	Match with the Referrer option in HTTP header.		
	<i>youtube-map</i>	Match Youtube content-id collection.		
	<i>youtube-id</i>	Match Youtube content-id.		
	<i>youku-id</i>	Match Youku content-id.		
	<i>hls-manifest</i>	Match with HLS manifest.		
	<i>dash-manifest</i>	Match with DASH manifest.		
	<i>hls-fragment</i>	Match HLS stream fragment.		
	<i>dash-fragment</i>	Match DASH stream fragment.		

config match-entries

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
pattern <string>	Pattern string for matching target (Referrer or URL pattern). For example, a, a*c, *a*, a*c*e, and *. Pattern strings.	string	Maximum length: 79	
target	Option in HTTP header or URL parameter to match.	option	-	path
	Option	Description		
	<i>path</i>	Match with the URL path.		
	<i>parameter</i>	Match with the URL parameters.		
	<i>referrer</i>	Match with the Referrer option in HTTP header.		
	<i>youtube-map</i>	Match Youtube content-id collection.		
	<i>youtube-id</i>	Match Youtube content-id.		
	<i>youku-id</i>	Match Youku content-id.		

config skip-entries

Parameter	Description	Type	Size	Default														
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295															
pattern <string>	Pattern string for matching target (Referrer or URL pattern). For example, a, a*c, *a*, a*c*e, and *. Pattern strings.	string	Maximum length: 79															
target	Option in HTTP header or URL parameter to match.	option	-	path														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>path</td><td>Match with the URL path.</td></tr><tr><td>parameter</td><td>Match with the URL parameters.</td></tr><tr><td>referrer</td><td>Match with the Referrer option in HTTP header.</td></tr><tr><td>youtube-map</td><td>Match Youtube content-id collection.</td></tr><tr><td>youtube-id</td><td>Match Youtube content-id.</td></tr><tr><td>youku-id</td><td>Match Youku content-id.</td></tr></table>				Option	Description	path	Match with the URL path.	parameter	Match with the URL parameters.	referrer	Match with the Referrer option in HTTP header.	youtube-map	Match Youtube content-id collection.	youtube-id	Match Youtube content-id.	youku-id	Match Youku content-id.
Option	Description																	
path	Match with the URL path.																	
parameter	Match with the URL parameters.																	
referrer	Match with the Referrer option in HTTP header.																	
youtube-map	Match Youtube content-id collection.																	
youtube-id	Match Youtube content-id.																	
youku-id	Match Youku content-id.																	

config wanopt peer



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R.

Configure WAN optimization peers.

```
config wanopt peer
  Description: Configure WAN optimization peers.
  edit <peer-host-id>
    set ip {ipv4-address-any}
  next
end
```

config wanopt peer

Parameter	Description	Type	Size	Default
ip	Peer IP address.	ipv4-address-any	Not Specified	0.0.0.0
peer-host-id	Peer host ID.	string	Maximum length: 35	

config wanopt profile



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R.

Configure WAN optimization profiles.

```
config wanopt profile
  Description: Configure WAN optimization profiles.
  edit <name>
    set auth-group {string}
    config cifs
      Description: Enable/disable CIFS (Windows sharing) WAN Optimization and configure CIFS
      WAN Optimization features.
      set byte-caching [enable|disable]
      set prefer-chunking [dynamic|fix]
      set protocol-opt [protocol|tcp]
      set secure-tunnel [enable|disable]
      set status [enable|disable]
      set tunnel-sharing [shared|express-shared|...]
    end
    set comments {var-string}
    config ftp
      Description: Enable/disable FTP WAN Optimization and configure FTP WAN Optimization
      features.
      set byte-caching [enable|disable]
      set prefer-chunking [dynamic|fix]
      set protocol-opt [protocol|tcp]
```

```

        set secure-tunnel [enable|disable]
        set status [enable|disable]
        set tunnel-sharing [shared|express-shared|...]
    end
    config http
        Description: Enable/disable HTTP WAN Optimization and configure HTTP WAN Optimization
features.
        set byte-caching [enable|disable]
        set prefer-chunking [dynamic|fix]
        set protocol-opt [protocol|tcp]
        set secure-tunnel [enable|disable]
        set ssl [enable|disable]
        set status [enable|disable]
        set tunnel-sharing [shared|express-shared|...]
    end
    config mapi
        Description: Enable/disable MAPI email WAN Optimization and configure MAPI WAN
Optimization features.
        set byte-caching [enable|disable]
        set secure-tunnel [enable|disable]
        set status [enable|disable]
        set tunnel-sharing [shared|express-shared|...]
    end
    config tcp
        Description: Enable/disable TCP WAN Optimization and configure TCP WAN Optimization
features.
        set byte-caching [enable|disable]
        set byte-caching-opt [mem-only|mem-disk]
        set port {user}
        set secure-tunnel [enable|disable]
        set ssl [enable|disable]
        set ssl-port {user}
        set status [enable|disable]
        set tunnel-sharing [shared|express-shared|...]
    end
    set transparent [enable|disable]
next
end

```

config wanopt profile

Parameter	Description	Type	Size	Default
auth-group	Optionally add an authentication group to restrict access to the WAN Optimization tunnel to peers in the authentication group.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
transparent	Enable/disable transparent mode.	option	-	enable
	Option	Description		
	<i>enable</i>	Determine if WAN Optimization changes client packet source addresses. Affects the routing configuration on the server network.		
	<i>disable</i>	Disable transparent mode. Client packets source addresses are changed to the source address of the FortiGate internal interface. Similar to source NAT.		

config cifs

Parameter	Description	Type	Size	Default						
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable byte-caching.	<i>disable</i>	Disable byte-caching.			
Option	Description									
<i>enable</i>	Enable byte-caching.									
<i>disable</i>	Disable byte-caching.									
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dynamic</i></td><td>Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.</td></tr><tr><td><i>fix</i></td><td>Select fixed data chunking.</td></tr></table>	Option	Description	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.	<i>fix</i>	Select fixed data chunking.			
Option	Description									
<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.									
<i>fix</i>	Select fixed data chunking.									
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>protocol</i></td><td>Using protocol-specific optimization.</td></tr><tr><td><i>tcp</i></td><td>Using generic TCP optimization.</td></tr></table>	Option	Description	<i>protocol</i>	Using protocol-specific optimization.	<i>tcp</i>	Using generic TCP optimization.			
Option	Description									
<i>protocol</i>	Using protocol-specific optimization.									
<i>tcp</i>	Using generic TCP optimization.									
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	Option	Description		
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		

config ftp

Parameter	Description	Type	Size	Default
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix
	Option	Description		
	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.		
	<i>fix</i>	Select fixed data chunking.		

Parameter	Description	Type	Size	Default								
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>protocol</i></td><td>Using protocol-specific optimization.</td></tr><tr><td><i>tcp</i></td><td>Using generic TCP optimization.</td></tr></table>	Option	Description	<i>protocol</i>	Using protocol-specific optimization.	<i>tcp</i>	Using generic TCP optimization.					
Option	Description											
<i>protocol</i>	Using protocol-specific optimization.											
<i>tcp</i>	Using generic TCP optimization.											
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-secured tunnelling.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-secured tunnelling.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-secured tunnelling.	<i>disable</i>	Disable SSL-secured tunnelling.					
Option	Description											
<i>enable</i>	Enable SSL-secured tunnelling.											
<i>disable</i>	Disable SSL-secured tunnelling.											
status	Enable/disable WAN Optimization.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WAN Optimization.</td></tr><tr><td><i>disable</i></td><td>Disable WAN Optimization.</td></tr></table>	Option	Description	<i>enable</i>	Enable WAN Optimization.	<i>disable</i>	Disable WAN Optimization.					
Option	Description											
<i>enable</i>	Enable WAN Optimization.											
<i>disable</i>	Disable WAN Optimization.											
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr></table>	Option	Description	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.			
Option	Description											
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.											
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.											
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.											

config http

Parameter	Description	Type	Size	Default
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix
	Option	Description		
	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.		
	<i>fix</i>	Select fixed data chunking.		
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol
	Option	Description		
	<i>protocol</i>	Using protocol-specific optimization.		
	<i>tcp</i>	Using generic TCP optimization.		
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL/TLS offloading.		
	<i>disable</i>	Disable SSL/TLS offloading.		
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		

Parameter	Description	Type	Size	Default								
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr></table>	Option	Description	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.			
Option	Description											
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.											
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.											
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.											

config mapi

Parameter	Description	Type	Size	Default						
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable byte-caching.	<i>disable</i>	Disable byte-caching.			
Option	Description									
<i>enable</i>	Enable byte-caching.									
<i>disable</i>	Disable byte-caching.									
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-secured tunnelling.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-secured tunnelling.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-secured tunnelling.	<i>disable</i>	Disable SSL-secured tunnelling.			
Option	Description									
<i>enable</i>	Enable SSL-secured tunnelling.									
<i>disable</i>	Disable SSL-secured tunnelling.									
status	Enable/disable WAN Optimization.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WAN Optimization.</td></tr><tr><td><i>disable</i></td><td>Disable WAN Optimization.</td></tr></table>	Option	Description	<i>enable</i>	Enable WAN Optimization.	<i>disable</i>	Disable WAN Optimization.			
Option	Description									
<i>enable</i>	Enable WAN Optimization.									
<i>disable</i>	Disable WAN Optimization.									
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		

config tcp

Parameter	Description	Type	Size	Default
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving it from the cache.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
byte-caching-opt	Select whether TCP byte-caching uses system memory only or both memory and disk space.	option	-	mem-only
	Option	Description		
	<i>mem-only</i>	Byte caching with memory only.		
	<i>mem-disk</i>	Byte caching with memory and disk.		
port	Port numbers or port number ranges for TCP. Only packets with a destination port number that matches this port number or range are accepted by this profile.	user	Not Specified	
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable SSL/TLS offloading.		
	<i>disable</i>	Disable SSL/TLS offloading.		
ssl-port	Port numbers or port number ranges on which to expect HTTPS traffic for SSL/TLS offloading.	user	Not Specified	
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	Option	Description		
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		

config wanopt remote-storage



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R.

Configure a remote cache device as Web cache storage.

```
config wanopt remote-storage
  Description: Configure a remote cache device as Web cache storage.
  set local-cache-id {string}
  set remote-cache-id {string}
  set remote-cache-ip {ipv4-address-any}
  set status [disable|enable]
end
```

config wanopt remote-storage

Parameter	Description	Type	Size	Default
local-cache-id	ID that this device uses to connect to the remote device.	string	Maximum length: 35	
remote-cache-id	ID of the remote device to which the device connects.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
remote-cache-ip	IP address of the remote device to which the device connects.	ipv4-address-any	Not Specified	0.0.0.0
status	Enable/disable using remote device as Web cache storage.	option	-	disable
		Option	Description	
		<i>disable</i>	Use local disks as Web cache storage.	
		<i>enable</i>	Use a remote device as Web cache storage.	

config wanopt settings



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R.

Configure WAN optimization settings.

```
config wanopt settings
  Description: Configure WAN optimization settings.
  set auto-detect-algorithm [simple|diff-req-resp]
  set host-id {string}
  set tunnel-optimization [memory-usage|balanced|...]
```



```

set tunnel-ssl-algorithm [high|medium|...]
end

```

config wanopt settings

Parameter	Description	Type	Size	Default								
auto-detect-algorithm	Auto detection algorithms used in tunnel negotiations.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Use the same TCP option value in SYN/SYNACK packets. Backward compatible.</td></tr><tr><td><i>diff-req-resp</i></td><td>Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.</td></tr></table>	Option	Description	<i>simple</i>	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.	<i>diff-req-resp</i>	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.					
Option	Description											
<i>simple</i>	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.											
<i>diff-req-resp</i>	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.											
host-id	Local host ID (must also be entered in the remote FortiGate's peer list).	string	Maximum length: 35	default-id								
tunnel-optimization	WANOpt tunnel optimization option.	option	-	balanced **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>memory-usage</i></td><td>Optimize tunnel for low system memory usage.</td></tr><tr><td><i>balanced</i></td><td>Optimize tunnel to balance between system memory usage and throughput.</td></tr><tr><td><i>throughput</i></td><td>Optimize tunnel for throughput.</td></tr></table>	Option	Description	<i>memory-usage</i>	Optimize tunnel for low system memory usage.	<i>balanced</i>	Optimize tunnel to balance between system memory usage and throughput.	<i>throughput</i>	Optimize tunnel for throughput.			
Option	Description											
<i>memory-usage</i>	Optimize tunnel for low system memory usage.											
<i>balanced</i>	Optimize tunnel to balance between system memory usage and throughput.											
<i>throughput</i>	Optimize tunnel for throughput.											
tunnel-ssl-algorithm	Relative strength of encryption algorithms accepted during tunnel negotiation.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.			
Option	Description											
<i>high</i>	High encryption. Allow only AES and ChaCha.											
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.											
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											

** Values may differ between models.

config wanopt webcache



This command is available for model(s): FortiGate 1000D, FortiGate 1001F, FortiGate 101F, FortiGate 1101E, FortiGate 121G, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3201F, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3701F, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 71F, FortiGate 800D, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 901G, FortiGate 91G, FortiGate-VM64 Aliyun, FortiGate-VM64 AWS, FortiGate-VM64 Azure, FortiGate-VM64 GCP, FortiGate-VM64 OPC, FortiGate-VM64, FortiGateRugged 70F 3G4G, FortiGateRugged 70F, FortiWiFi 80F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G DSL, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000F, FortiGate 100F, FortiGate 1100E, FortiGate 120G, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3200F, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3700F, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 80F Bypass, FortiGate 80F DSL, FortiGate 80F-POE, FortiGate 80F, FortiGate 900G, FortiGate 90G, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R.

Configure global Web cache settings.

```
config wanopt webcache
  Description: Configure global Web cache settings.
  set always-revalidate [enable|disable]
  set cache-by-default [enable|disable]
  set cache-cookie [enable|disable]
  set cache-expired [enable|disable]
  set default-ttl {integer}
  set external [enable|disable]
  set fresh-factor {integer}
  set host-validate [enable|disable]
  set ignore-conditional [enable|disable]
  set ignore-ie-reload [enable|disable]
  set ignore-ims [enable|disable]
  set ignore-pnc [enable|disable]
  set max-object-size {integer}
  set max-ttl {integer}
  set min-ttl {integer}
  set neg-resp-time {integer}
  set reval-pnc [enable|disable]
end
```

config wanopt webcache

Parameter	Description	Type	Size	Default						
always-revalidate	Enable/disable revalidation of requested cached objects, which have content on the server, before serving it to the client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable revalidation of requested cached objects.</td></tr><tr><td><i>disable</i></td><td>Disable revalidation of requested cached objects.</td></tr></table>	Option	Description	<i>enable</i>	Enable revalidation of requested cached objects.	<i>disable</i>	Disable revalidation of requested cached objects.			
Option	Description									
<i>enable</i>	Enable revalidation of requested cached objects.									
<i>disable</i>	Disable revalidation of requested cached objects.									
cache-by-default	Enable/disable caching content that lacks explicit caching policies from the server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable caching content that lacks explicit caching policies.</td></tr><tr><td><i>disable</i></td><td>Disable caching content that lacks explicit caching policies.</td></tr></table>	Option	Description	<i>enable</i>	Enable caching content that lacks explicit caching policies.	<i>disable</i>	Disable caching content that lacks explicit caching policies.			
Option	Description									
<i>enable</i>	Enable caching content that lacks explicit caching policies.									
<i>disable</i>	Disable caching content that lacks explicit caching policies.									
cache-cookie	Enable/disable caching cookies. Since cookies contain information for or about individual users, they not usually cached.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Cache cookies.</td></tr><tr><td><i>disable</i></td><td>Do not cache cookies.</td></tr></table>	Option	Description	<i>enable</i>	Cache cookies.	<i>disable</i>	Do not cache cookies.			
Option	Description									
<i>enable</i>	Cache cookies.									
<i>disable</i>	Do not cache cookies.									
cache-expired	Enable/disable caching type-1 objects that are already expired on arrival.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-ttl	Default object expiry time (default = 1440 min (1 day); maximum = 5256000 min (10 years)). This only applies to those objects that do not have an expiry time set by the web server.	integer	Minimum value: 1440 Maximum value: 5256000							
external	Enable/disable external Web caching.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable external Web caching.</td></tr><tr><td><i>disable</i></td><td>Disable external Web caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable external Web caching.	<i>disable</i>	Disable external Web caching.			
Option	Description									
<i>enable</i>	Enable external Web caching.									
<i>disable</i>	Disable external Web caching.									

Parameter	Description	Type	Size	Default						
fresh-factor	Frequency that the server is checked to see if any objects have expired (1 - 100, default = 100). The higher the fresh factor, the less often the checks occur.	integer	Minimum value: 1 Maximum value: 100	100						
host-validate	Enable/disable validating "Host:" with original server IP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable validating "Host:" with original server IP.</td></tr><tr><td><i>disable</i></td><td>Disable validating "Host:" with original server IP.</td></tr></table>	Option	Description	<i>enable</i>	Enable validating "Host:" with original server IP.	<i>disable</i>	Disable validating "Host:" with original server IP.			
Option	Description									
<i>enable</i>	Enable validating "Host:" with original server IP.									
<i>disable</i>	Disable validating "Host:" with original server IP.									
ignore-conditional	Enable/disable controlling the behavior of cache-control HTTP 1.1 header values.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring cache-control HTTP 1.1 header values.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring cache-control HTTP 1.1 header values.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring cache-control HTTP 1.1 header values.	<i>disable</i>	Disable ignoring cache-control HTTP 1.1 header values.			
Option	Description									
<i>enable</i>	Enable ignoring cache-control HTTP 1.1 header values.									
<i>disable</i>	Disable ignoring cache-control HTTP 1.1 header values.									
ignore-ie-reload	Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.</td></tr><tr><td><i>disable</i></td><td>Disable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.</td></tr></table>	Option	Description	<i>enable</i>	Enable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	<i>disable</i>	Disable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.			
Option	Description									
<i>enable</i>	Enable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.									
<i>disable</i>	Disable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.									
ignore-ims	Enable/disable ignoring the if-modified-since (IMS) header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring the if-modified-since (IMS) header.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring the if-modified-since (IMS) header.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring the if-modified-since (IMS) header.	<i>disable</i>	Disable ignoring the if-modified-since (IMS) header.			
Option	Description									
<i>enable</i>	Enable ignoring the if-modified-since (IMS) header.									
<i>disable</i>	Disable ignoring the if-modified-since (IMS) header.									
ignore-pnc	Enable/disable ignoring the pragma no-cache (PNC) header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring the pragma no-cache (PNC) header.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring the pragma no-cache (PNC) header.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring the pragma no-cache (PNC) header.	<i>disable</i>	Disable ignoring the pragma no-cache (PNC) header.			
Option	Description									
<i>enable</i>	Enable ignoring the pragma no-cache (PNC) header.									
<i>disable</i>	Disable ignoring the pragma no-cache (PNC) header.									

Parameter	Description	Type	Size	Default
max-object-size	Maximum cacheable object size in kB (1 - 2147483 kb (2GB). All objects that exceed this are delivered to the client but not stored in the web cache.	integer	Minimum value: 1 Maximum value: 2147483	512000
max-ttl	Maximum time an object can stay in the web cache without checking to see if it has expired on the server (default = 7200 min (5 days); maximum = 5256000 min (10 years)).	integer	Minimum value: 1 Maximum value: 5256000	7200
min-ttl	Minimum time an object can stay in the web cache without checking to see if it has expired on the server (default = 5 min; maximum = 5256000 (10 years)).	integer	Minimum value: 1 Maximum value: 5256000	5
neg-resp-time	Time in minutes to cache negative responses or errors (0 - 4294967295, default = 0 which means negative responses are not cached).	integer	Minimum value: 0 Maximum value: 4294967295	0
reval-pnc	Enable/disable revalidation of pragma-no-cache (PNC) to address bandwidth concerns.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable revalidation of pragma-no-cache (PNC).	
		<i>disable</i>	Disable revalidation of pragma-no-cache (PNC).	

web-proxy

This section includes syntax for the following commands:

- [config web-proxy debug-url on page 2350](#)
- [config web-proxy explicit on page 2351](#)
- [config web-proxy fast-fallback on page 2358](#)
- [config web-proxy forward-server-group on page 2362](#)
- [config web-proxy forward-server on page 2359](#)
- [config web-proxy global on page 2363](#)
- [config web-proxy isolator-server on page 2368](#)
- [config web-proxy profile on page 2369](#)
- [config web-proxy url-match on page 2374](#)
- [config web-proxy wisp on page 2375](#)

config web-proxy debug-url

Configure debug URL addresses.

```
config web-proxy debug-url
  Description: Configure debug URL addresses.
  edit <name>
    set exact [enable|disable]
    set status [enable|disable]
    set url-pattern {string}
  next
end
```

config web-proxy debug-url

Parameter	Description	Type	Size	Default
exact	Enable/disable matching the exact path.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable matching the exact path.		
	<i>disable</i>	Disable matching the exact path.		
name	Debug URL name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
status	Enable/disable this URL exemption.	option	-	enable
	Option	Description		
	enable	Enable this URL exemption.		
	disable	Disable this URL exemption.		
url-pattern	URL exemption pattern.	string	Maximum length: 511	

config web-proxy explicit

Configure explicit Web proxy settings.

```
config web-proxy explicit
  Description: Configure explicit Web proxy settings.
  set client-cert [disable|enable]
  set empty-cert-action [accept|block|...]
  set ftp-incoming-port {user}
  set ftp-over-http [enable|disable]
  set http-connection-mode [static|multiplex|...]
  set http-incoming-port {user}
  set https-incoming-port {user}
  set https-replacement-message [enable|disable]
  set incoming-ip {ipv4-address-any}
  set incoming-ip6 {ipv6-address}
  set interface {string}
  set interface-select-method [sdwan|specify]
  set ipv6-status [enable|disable]
  set message-upon-server-error [enable|disable]
  set outgoing-ip {ipv4-address-any}
  set outgoing-ip6 {ipv6-address}
  set pac-file-data {user}
  set pac-file-name {string}
  set pac-file-server-port {user}
  set pac-file-server-status [enable|disable]
  set pac-file-through-https [enable|disable]
  set pac-file-url {user}
config pac-policy
  Description: PAC policies.
  edit <policyid>
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set pac-file-data {user}
    set pac-file-name {string}
    set srcaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set status [enable|disable]
```

```

    next
end
set pref-dns-result [ipv4|ipv6|...]
set realm {string}
set sec-default-action [accept|deny]
set secure-web-proxy [disable|enable|...]
set secure-web-proxy-cert <name1>, <name2>, ...
set socks [enable|disable]
set socks-incoming-port {user}
set ssl-algorithm [high|medium|...]
set ssl-dh-bits [768|1024|...]
set status [enable|disable]
set strict-guest [enable|disable]
set trace-auth-no-rsp [enable|disable]
set unknown-http-version [reject|best-effort]
set user-agent-detect [disable|enable]
set vrf-select {integer}
end

```

config web-proxy explicit

Parameter	Description	Type	Size	Default
client-cert	Enable/disable to request client certificate.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable client certificate request.		
	<i>enable</i>	Enable client certificate request.		
empty-cert-action	Action of an empty client certificate.	option	-	block
	Option	Description		
	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.		
	<i>block</i>	Block the SSL handshake if the client certificate is empty.		
	<i>accept-unmanageable</i>	Accept the SSL handshake only if the end-point is unmanageable.		
ftp-incoming-port	Accept incoming FTP-over-HTTP requests on one or more ports (0 - 65535, default = 0; use the same as HTTP).	user	Not Specified	
ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FTP-over-HTTP sessions.</td></tr><tr><td><i>disable</i></td><td>Disable FTP-over-HTTP sessions.</td></tr></table>	Option	Description	<i>enable</i>	Enable FTP-over-HTTP sessions.	<i>disable</i>	Disable FTP-over-HTTP sessions.					
	Option	Description										
	<i>enable</i>	Enable FTP-over-HTTP sessions.										
<i>disable</i>	Disable FTP-over-HTTP sessions.											
http-connection-mode	HTTP connection mode (default = static).	option	-	static								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Only one server connection exists during the proxy session.</td></tr><tr><td><i>multiplex</i></td><td>Established connections are held until the proxy session ends.</td></tr><tr><td><i>serverpool</i></td><td>Established connections are shared with other proxy sessions.</td></tr></table>	Option	Description	<i>static</i>	Only one server connection exists during the proxy session.	<i>multiplex</i>	Established connections are held until the proxy session ends.	<i>serverpool</i>	Established connections are shared with other proxy sessions.			
	Option	Description										
	<i>static</i>	Only one server connection exists during the proxy session.										
	<i>multiplex</i>	Established connections are held until the proxy session ends.										
<i>serverpool</i>	Established connections are shared with other proxy sessions.											
http-incoming-port	Accept incoming HTTP requests on one or more ports (0 - 65535, default = 8080).	user	Not Specified									
https-incoming-port	Accept incoming HTTPS requests on one or more ports (0 - 65535, default = 0, use the same as HTTP).	user	Not Specified									
https-replacement-message	Enable/disable sending the client a replacement message for HTTPS requests.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display a replacement message for HTTPS requests.</td></tr><tr><td><i>disable</i></td><td>Do not display a replacement message for HTTPS requests.</td></tr></table>	Option	Description	<i>enable</i>	Display a replacement message for HTTPS requests.	<i>disable</i>	Do not display a replacement message for HTTPS requests.					
	Option	Description										
	<i>enable</i>	Display a replacement message for HTTPS requests.										
<i>disable</i>	Do not display a replacement message for HTTPS requests.											
incoming-ip	Restrict the explicit HTTP proxy to only accept sessions from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0								
incoming-ip6	Restrict the explicit web proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	sdwan								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr></table>	Option	Description	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.							
	Option	Description										
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>specify</i>	Set outgoing interface manually.					
	Option	Description								
<i>specify</i>	Set outgoing interface manually.									
ipv6-status	Enable/disable allowing an IPv6 web proxy destination in policies and all IPv6 related entries in this command.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowing an IPv6 web proxy destination.</td></tr><tr><td><i>disable</i></td><td>Disable allowing an IPv6 web proxy destination.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowing an IPv6 web proxy destination.	<i>disable</i>	Disable allowing an IPv6 web proxy destination.			
	Option	Description								
	<i>enable</i>	Enable allowing an IPv6 web proxy destination.								
<i>disable</i>	Disable allowing an IPv6 web proxy destination.									
message-upon-server-error	Enable/disable displaying a replacement message when a server error is detected.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display a replacement message when a server error is detected.</td></tr><tr><td><i>disable</i></td><td>Do not display a replacement message when a server error is detected.</td></tr></table>	Option	Description	<i>enable</i>	Display a replacement message when a server error is detected.	<i>disable</i>	Do not display a replacement message when a server error is detected.			
	Option	Description								
	<i>enable</i>	Display a replacement message when a server error is detected.								
<i>disable</i>	Do not display a replacement message when a server error is detected.									
outgoing-ip	Outgoing HTTP requests will have this IP address as their source address. An interface must have this IP address.	ipv4-address-any	Not Specified							
outgoing-ip6	Outgoing HTTP requests will leave this IPv6. Multiple interfaces can be specified. Interfaces must have these IPv6 addresses.	ipv6-address	Not Specified							
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified							
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac						
pac-file-server-port	Port number that PAC traffic from client web browsers uses to connect to the explicit web proxy (0 - 65535, default = 0; use the same as HTTP).	user	Not Specified							
pac-file-server-status	Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Proxy Auto-Configuration (PAC).</td></tr><tr><td><i>disable</i></td><td>Disable Proxy Auto-Configuration (PAC).</td></tr></table>	Option	Description	<i>enable</i>	Enable Proxy Auto-Configuration (PAC).	<i>disable</i>	Disable Proxy Auto-Configuration (PAC).			
	Option	Description								
	<i>enable</i>	Enable Proxy Auto-Configuration (PAC).								
<i>disable</i>	Disable Proxy Auto-Configuration (PAC).									

Parameter	Description	Type	Size	Default										
pac-file-through-https	Enable/disable to get Proxy Auto-Configuration (PAC) through HTTPS.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable to get Proxy Auto-Configuration (PAC) through HTTPS.</td></tr><tr><td>disable</td><td>Disable to get Proxy Auto-Configuration (PAC) through HTTPS.</td></tr></table>	Option	Description	enable	Enable to get Proxy Auto-Configuration (PAC) through HTTPS.	disable	Disable to get Proxy Auto-Configuration (PAC) through HTTPS.							
Option	Description													
enable	Enable to get Proxy Auto-Configuration (PAC) through HTTPS.													
disable	Disable to get Proxy Auto-Configuration (PAC) through HTTPS.													
pac-file-url	PAC file access URL. Read-only.	user	Not Specified											
pref-dns-result	Prefer resolving addresses using the configured IPv4 or IPv6 DNS server (default = ipv4).	option	-	ipv4										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>Send the IPv4 request first and then the IPv6 request. Use the DNS response that returns to the FortiGate first.</td></tr><tr><td>ipv6</td><td>Send the IPv6 request first and then the IPv4 request. Use the DNS response that returns to the FortiGate first.</td></tr><tr><td>ipv4-strict</td><td>Use the IPv4 DNS response. If the IPv6 DNS response arrives first, wait 50ms for the IPv4 response and then use the IPv4 response, otherwise the IPv6.</td></tr><tr><td>ipv6-strict</td><td>Use the IPv6 DNS response. If the IPv4 DNS response arrives first, wait 50ms for the IPv6 response and then use the IPv6 response, otherwise the IPv4.</td></tr></table>	Option	Description	ipv4	Send the IPv4 request first and then the IPv6 request. Use the DNS response that returns to the FortiGate first.	ipv6	Send the IPv6 request first and then the IPv4 request. Use the DNS response that returns to the FortiGate first.	ipv4-strict	Use the IPv4 DNS response. If the IPv6 DNS response arrives first, wait 50ms for the IPv4 response and then use the IPv4 response, otherwise the IPv6.	ipv6-strict	Use the IPv6 DNS response. If the IPv4 DNS response arrives first, wait 50ms for the IPv6 response and then use the IPv6 response, otherwise the IPv4.			
Option	Description													
ipv4	Send the IPv4 request first and then the IPv6 request. Use the DNS response that returns to the FortiGate first.													
ipv6	Send the IPv6 request first and then the IPv4 request. Use the DNS response that returns to the FortiGate first.													
ipv4-strict	Use the IPv4 DNS response. If the IPv6 DNS response arrives first, wait 50ms for the IPv4 response and then use the IPv4 response, otherwise the IPv6.													
ipv6-strict	Use the IPv6 DNS response. If the IPv4 DNS response arrives first, wait 50ms for the IPv6 response and then use the IPv6 response, otherwise the IPv4.													
realm	Authentication realm used to identify the explicit web proxy (maximum of 63 characters).	string	Maximum length: 63	default										
sec-default-action	Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.	option	-	deny										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>accept</td><td>Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.</td></tr><tr><td>deny</td><td>Deny requests unless there is a matching explicit web proxy policy.</td></tr></table>	Option	Description	accept	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.	deny	Deny requests unless there is a matching explicit web proxy policy.							
Option	Description													
accept	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.													
deny	Deny requests unless there is a matching explicit web proxy policy.													
secure-web-proxy	Enable/disable/require the secure web proxy for HTTP and HTTPS session.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable secure webproxy.</td></tr><tr><td>enable</td><td>Enable secure webproxy access.</td></tr></table>	Option	Description	disable	Disable secure webproxy.	enable	Enable secure webproxy access.							
Option	Description													
disable	Disable secure webproxy.													
enable	Enable secure webproxy access.													

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>secure</i>	Require secure webproxy access.		
secure-web-proxy-cert <name>	Name of certificates for secure web proxy. Certificate list.	string	Maximum length: 79	
socks	Enable/disable the SOCKS proxy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the SOCKS proxy.		
	<i>disable</i>	Disable the SOCKS proxy.		
socks-incoming-port	Accept incoming SOCKS proxy requests on one or more ports (0 - 65535, default = 0; use the same as HTTP).	user	Not Specified	
ssl-algorithm	Relative strength of encryption algorithms accepted in HTTPS deep scan: high, medium, or low.	option	-	low
	Option	Description		
	<i>high</i>	High encryption. Allow only AES and ChaCha.		
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
ssl-dh-bits	Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).	option	-	2048
	Option	Description		
	<i>768</i>	768-bit Diffie-Hellman prime.		
	<i>1024</i>	1024-bit Diffie-Hellman prime.		
	<i>1536</i>	1536-bit Diffie-Hellman prime.		
	<i>2048</i>	2048-bit Diffie-Hellman prime.		
status	Enable/disable the explicit Web proxy for HTTP and HTTPS session.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the explicit web proxy.		
	<i>disable</i>	Disable the explicit web proxy.		

Parameter	Description	Type	Size	Default						
strict-guest	Enable/disable strict guest user checking by the explicit web proxy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict guest user checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict guest user checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict guest user checking.	<i>disable</i>	Disable strict guest user checking.			
Option	Description									
<i>enable</i>	Enable strict guest user checking.									
<i>disable</i>	Disable strict guest user checking.									
trace-auth-no-rsp	Enable/disable logging timed-out authentication requests.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging timed-out authentication requests.</td></tr><tr><td><i>disable</i></td><td>Disable logging timed-out authentication requests.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging timed-out authentication requests.	<i>disable</i>	Disable logging timed-out authentication requests.			
Option	Description									
<i>enable</i>	Enable logging timed-out authentication requests.									
<i>disable</i>	Disable logging timed-out authentication requests.									
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reject</i></td><td>Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.</td></tr><tr><td><i>best-effort</i></td><td>Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.</td></tr></table>	Option	Description	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.			
Option	Description									
<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.									
<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.									
user-agent-detect	Enable/disable to detect device type by HTTP user-agent if no client certificate provided.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable to detect unknown device by HTTP user-agent if no client certificate provided.</td></tr><tr><td><i>enable</i></td><td>Enable to detect unknown device by HTTP user-agent if no client certificate provided.</td></tr></table>	Option	Description	<i>disable</i>	Disable to detect unknown device by HTTP user-agent if no client certificate provided.	<i>enable</i>	Enable to detect unknown device by HTTP user-agent if no client certificate provided.			
Option	Description									
<i>disable</i>	Disable to detect unknown device by HTTP user-agent if no client certificate provided.									
<i>enable</i>	Enable to detect unknown device by HTTP user-agent if no client certificate provided.									
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	-1						

config pac-policy

Parameter	Description	Type	Size	Default
comments	Optional comments.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79	
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
policyid	Policy ID.	integer	Minimum value: 1 Maximum value: 100	0
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Source address6 objects. Address name.	string	Maximum length: 79	
status	Enable/disable policy.	option	-	enable
		Option	Description	
		enable	Enable policy.	
		disable	Disable policy.	

config web-proxy fast-fallback

Proxy destination connection fast-fallback.

```
config web-proxy fast-fallback
  Description: Proxy destination connection fast-fallback.
  edit <name>
    set connection-mode [sequentially|simultaneously]
    set connection-timeout {integer}
    set protocol [IPv4-first|IPv6-first|...]
    set status [enable|disable]
  next
end
```

config web-proxy fast-fallback

Parameter	Description	Type	Size	Default
connection-mode	Connection mode for multiple destinations.	option	-	sequentially
	Option	Description		
	<i>sequentially</i>	Connect the different destinations sequentially.		
	<i>simultaneously</i>	Connect the different destinations simultaneously.		
connection-timeout	Number of milliseconds to wait before starting another connection (200 - 1800000, default = 200). For sequential connection-mode only.	integer	Minimum value: 200 Maximum value: 1800000	200
name	Configure a name for the fast-fallback entry.	string	Maximum length: 63	
protocol	Connection protocols for multiple destinations.	option	-	IPv4-first
	Option	Description		
	<i>IPv4-first</i>	Connect IPv4 destinations first.		
	<i>IPv6-first</i>	Connect IPv6 destinations first.		
	<i>IPv4-only</i>	Connect IPv4 destinations only.		
	<i>IPv6-only</i>	Connect IPv6 destinations only.		
status	Enable/disable the fast-fallback entry.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Status of the entry.		
	<i>disable</i>	Disable Status of the entry.		

config web-proxy forward-server

Configure forward-server addresses.

```
config web-proxy forward-server
  Description: Configure forward-server addresses.
  edit <name>
    set addr-type [ip|ipv6|...]
    set comment {string}
    set fqdn {string}
```

```

set healthcheck [disable|enable]
set interface {string}
set interface-select-method [sdwan|specify]
set ip {ipv4-address-any}
set ipv6 {ipv6-address}
set masquerade [enable|disable]
set monitor {string}
set password {password}
set port {integer}
set server-down-option [block|pass]
set username {string}
set vrf-select {integer}
next
end

```

config web-proxy forward-server

Parameter	Description	Type	Size	Default
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip
	Option	Description		
	<i>ip</i>	Use an IPv4 address for the forwarding proxy server.		
	<i>ipv6</i>	Use an IPv6 address for the forwarding proxy server.		
	<i>fqdn</i>	Use the FQDN for the forwarding proxy server.		
comment	Comment.	string	Maximum length: 63	
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255	
healthcheck	Enable/disable forward server health checking. Attempts to connect through the remote forwarding server to a destination to verify that the forwarding server is operating normally.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable health checking.		
	<i>enable</i>	Enable health checking.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default						
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	sdwan						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description									
sdwan	Set outgoing interface by SD-WAN or policy routing rules.									
specify	Set outgoing interface manually.									
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified	0.0.0.0						
ipv6	Forward proxy server IPv6 address.	ipv6-address	Not Specified	::						
masquerade	Enable/disable use of the of the IP address of the outgoing interface as the client IP address (default = enable)	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of the IP address of the outgoing interface as the client IP address.</td></tr><tr><td>disable</td><td>Disable use of the of the IP address of the outgoing interface as the client IP address.</td></tr></table>	Option	Description	enable	Enable use of the IP address of the outgoing interface as the client IP address.	disable	Disable use of the of the IP address of the outgoing interface as the client IP address.			
Option	Description									
enable	Enable use of the IP address of the outgoing interface as the client IP address.									
disable	Disable use of the of the IP address of the outgoing interface as the client IP address.									
monitor	URL for forward server health check monitoring (default = www.google.com).	string	Maximum length: 255	www.google.com						
name	Server name.	string	Maximum length: 63							
password	HTTP authentication password.	password	Not Specified							
port	Port number that the forwarding server expects to receive HTTP sessions on (1 - 65535, default = 3128).	integer	Minimum value: 1 Maximum value: 65535	3128						
server-down-option	Action to take when the forward server is found to be down: block sessions until the server is back up or pass sessions to their destination.	option	-	block						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>block</td><td>Block sessions until the server is back up.</td></tr><tr><td>pass</td><td>Pass sessions to their destination bypassing the forward server.</td></tr></table>	Option	Description	block	Block sessions until the server is back up.	pass	Pass sessions to their destination bypassing the forward server.			
Option	Description									
block	Block sessions until the server is back up.									
pass	Pass sessions to their destination bypassing the forward server.									

Parameter	Description	Type	Size	Default
username	HTTP authentication user name.	string	Maximum length: 64	
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	-1

config web-proxy forward-server-group

Configure a forward server group consisting of multiple forward servers. Supports failover and load balancing.

```

config web-proxy forward-server-group
    Description: Configure a forward server group consisting of multiple forward servers. Supports
    failover and load balancing.
    edit <name>
        set affinity [enable|disable]
        set group-down-option [block|pass]
        set ldb-method [weighted|least-session|...]
        config server-list
            Description: Add web forward servers to a list to form a server group. Optionally
            assign weights to each server.
            edit <name>
                set weight {integer}
            next
        end
    next
end

```

config web-proxy forward-server-group

Parameter	Description	Type	Size	Default
affinity	Enable/disable affinity, attaching a source-ip's traffic to the assigned forwarding server until the forward-server-affinity-timeout is reached (under web-proxy global).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable affinity.		
	<i>disable</i>	Disable affinity.		

Parameter	Description	Type	Size	Default								
group-down-option	Action to take when all of the servers in the forward server group are down: block sessions until at least one server is back up or pass sessions to their destination.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block sessions until at least one server in the group is back up.</td></tr><tr><td><i>pass</i></td><td>Pass sessions to their destination bypassing servers in the forward server group.</td></tr></table>	Option	Description	<i>block</i>	Block sessions until at least one server in the group is back up.	<i>pass</i>	Pass sessions to their destination bypassing servers in the forward server group.					
Option	Description											
<i>block</i>	Block sessions until at least one server in the group is back up.											
<i>pass</i>	Pass sessions to their destination bypassing servers in the forward server group.											
ldb-method	Load balance method: weighted or least-session.	option	-	weighted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weighted</i></td><td>Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.</td></tr><tr><td><i>least-session</i></td><td>Send new sessions to the server with lowest session count.</td></tr><tr><td><i>active-passive</i></td><td>Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.</td></tr></table>	Option	Description	<i>weighted</i>	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.	<i>least-session</i>	Send new sessions to the server with lowest session count.	<i>active-passive</i>	Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.			
Option	Description											
<i>weighted</i>	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.											
<i>least-session</i>	Send new sessions to the server with lowest session count.											
<i>active-passive</i>	Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.											
name	Configure a forward server group consisting one or multiple forward servers. Supports failover and load balancing.	string	Maximum length: 63									

config server-list

Parameter	Description	Type	Size	Default
name	Forward server name.	string	Maximum length: 63	
weight	Optionally assign a weight of the forwarding server for weighted load balancing (1 - 100, default = 10).	integer	Minimum value: 1 Maximum value: 100	10

config web-proxy global

Configure Web proxy global settings.

```
config web-proxy global
  Description: Configure Web proxy global settings.
  set always-learn-client-ip [enable|disable]
```

```

set fast-policy-match [enable|disable]
set forward-proxy-auth [enable|disable]
set forward-server-affinity-timeout {integer}
set http2-client-window-size {integer}
set http2-server-window-size {integer}
set ldap-user-cache [enable|disable]
set learn-client-ip [enable|disable]
set learn-client-ip-from-header {option1}, {option2}, ...
set learn-client-ip-srcaddr <name1>, <name2>, ...
set learn-client-ip-srcaddr6 <name1>, <name2>, ...
set log-app-id [enable|disable]
set log-forward-server [enable|disable]
set log-policy-pending [enable|disable]
set max-message-length {integer}
set max-request-length {integer}
set max-waf-body-cache-length {integer}
set proxy-fqdn {string}
set proxy-transparent-cert-inspection [enable|disable]
set request-obs-fold [replace-with-sp|block|...]
set src-affinity-exempt-addr {ipv4-address-any}
set src-affinity-exempt-addr6 {ipv6-address}
set ssl-ca-cert {string}
set ssl-cert {string}
set strict-web-check [enable|disable]
set webproxy-profile {string}
end

```

end

config web-proxy global

Parameter	Description	Type	Size	Default						
always-learn-client-ip	Enable/disable learning the client's IP address from headers for every request.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable learning the client's IP address from headers for every request.</td></tr><tr><td><i>disable</i></td><td>Disable learning the client's IP address from headers for every request.</td></tr></table>	Option	Description	<i>enable</i>	Enable learning the client's IP address from headers for every request.	<i>disable</i>	Disable learning the client's IP address from headers for every request.			
Option	Description									
<i>enable</i>	Enable learning the client's IP address from headers for every request.									
<i>disable</i>	Disable learning the client's IP address from headers for every request.									
fast-policy-match	Enable/disable fast matching algorithm for explicit and transparent proxy policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
forward-proxy-auth	Enable/disable forwarding proxy authentication headers.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forwarding proxy authentication headers.</td></tr><tr><td><i>disable</i></td><td>Disable forwarding proxy authentication headers.</td></tr></table>	Option	Description	<i>enable</i>	Enable forwarding proxy authentication headers.	<i>disable</i>	Disable forwarding proxy authentication headers.			
	Option	Description								
	<i>enable</i>	Enable forwarding proxy authentication headers.								
<i>disable</i>	Disable forwarding proxy authentication headers.									
forward-server-affinity-timeout	Period of time before the source IP's traffic is no longer assigned to the forwarding server (6 - 60 min, default = 30).	integer	Minimum value: 6 Maximum value: 60	30						
http2-client-window-size	HTTP/2 client initial window size in bytes (65535 - 2147483647, default = 1048576 (1MB)).	integer	Minimum value: 65535 Maximum value: 2147483647	1048576						
http2-server-window-size	HTTP/2 server initial window size in bytes (65535 - 2147483647, default = 1048576 (1MB)).	integer	Minimum value: 65535 Maximum value: 2147483647	1048576						
ldap-user-cache	Enable/disable LDAP user cache for explicit and transparent proxy user.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
learn-client-ip	Enable/disable learning the client's IP address from headers.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable learning the client's IP address from headers.</td></tr><tr><td><i>disable</i></td><td>Disable learning the client's IP address from headers.</td></tr></table>	Option	Description	<i>enable</i>	Enable learning the client's IP address from headers.	<i>disable</i>	Disable learning the client's IP address from headers.			
	Option	Description								
	<i>enable</i>	Enable learning the client's IP address from headers.								
<i>disable</i>	Disable learning the client's IP address from headers.									
learn-client-ip-from-header	Learn client IP address from the specified headers.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>true-client-ip</i></td><td>Learn the client IP address from the True-Client-IP header.</td></tr><tr><td><i>x-real-ip</i></td><td>Learn the client IP address from the X-Real-IP header.</td></tr></table>	Option	Description	<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.	<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.			
	Option	Description								
	<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.								
<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>x-forwarded-for</i></td><td>Learn the client IP address from the X-Forwarded-For header.</td></tr></table>	Option	Description	<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.					
Option	Description									
<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.									
learn-client-ip-srcaddr <name>	Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79							
learn-client-ip-srcaddr6 <name>	IPv6 Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79							
log-app-id	Enable/disable always log application type in traffic log.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging application type in traffic log.</td></tr><tr><td><i>disable</i></td><td>Disable logging application type in traffic log.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging application type in traffic log.	<i>disable</i>	Disable logging application type in traffic log.			
Option	Description									
<i>enable</i>	Enable logging application type in traffic log.									
<i>disable</i>	Disable logging application type in traffic log.									
log-forward-server	Enable/disable forward server name logging in forward traffic log.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging forward server name in forward traffic log.</td></tr><tr><td><i>disable</i></td><td>Disable logging forward server name in forward traffic log.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging forward server name in forward traffic log.	<i>disable</i>	Disable logging forward server name in forward traffic log.			
Option	Description									
<i>enable</i>	Enable logging forward server name in forward traffic log.									
<i>disable</i>	Disable logging forward server name in forward traffic log.									
log-policy-pending	Enable/disable logging sessions that are pending on policy matching.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging sessions that are pending on policy matching.</td></tr><tr><td><i>disable</i></td><td>Disable logging sessions that are pending on policy matching.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging sessions that are pending on policy matching.	<i>disable</i>	Disable logging sessions that are pending on policy matching.			
Option	Description									
<i>enable</i>	Enable logging sessions that are pending on policy matching.									
<i>disable</i>	Disable logging sessions that are pending on policy matching.									
max-message-length	Maximum length of HTTP message, not including body (16 - 256 Kbytes, default = 32).	integer	Minimum value: 16 Maximum value: 256	32						
max-request-length	Maximum length of HTTP request line (2 - 64 Kbytes, default = 8).	integer	Minimum value: 2 Maximum value: 64	8						

Parameter	Description	Type	Size	Default
max-waf-body-cache-length	Maximum length of HTTP messages processed by Web Application Firewall (WAF) (1 - 1024 Kbytes, default = 1).	integer	Minimum value: 1 Maximum value: 1024	1
proxy-fqdn	Fully Qualified Domain Name of the explicit web proxy (default = default.fqdn) that clients connect to.	string	Maximum length: 255	default.fqdn
proxy-transparent-cert-inspection	Enable/disable transparent proxy certificate inspection.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable proxying certificate inspection in transparent mode.	
	<i>disable</i>		Disable proxying certificate inspection in transparent mode.	
request-obs-fold	Action when HTTP/1.x request header contains obs-fold.	option	-	keep
	Option		Description	
	<i>replace-with-sp</i>		Replace CRLF in obs-fold with SP in the request header for HTTP/1.x.	
	<i>block</i>		Block HTTP/1.x request with obs-fold.	
	<i>keep</i>		Keep obs-fold in the request header for HTTP/1.x. There are known security risks.	
src-affinity-exempt-addr	IPv4 source addresses to exempt proxy affinity.	ipv4-address-any	Not Specified	
src-affinity-exempt-addr6	IPv6 source addresses to exempt proxy affinity.	ipv6-address	Not Specified	
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35	Fortinet_CA_SSL
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35	Fortinet_Factory
strict-web-check	Enable/disable strict web checking to block web sites that send incorrect headers that don't conform to HTTP.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable strict web checking.		
	<i>disable</i>	Disable strict web checking.		
webproxy-profile	Name of the web proxy profile to apply when explicit proxy traffic is allowed by default and traffic is accepted that does not match an explicit proxy policy.	string	Maximum length: 63	

config web-proxy isolator-server

Configure forward-server addresses.

```

config web-proxy isolator-server
  Description: Configure forward-server addresses.
  edit <name>
    set addr-type [ip|ipv6|...]
    set comment {string}
    set fqdn {string}
    set interface {string}
    set interface-select-method [sdwan|specify]
    set ip {ipv4-address-any}
    set ipv6 {ipv6-address}
    set masquerade [enable|disable]
    set port {integer}
    set vrf-select {integer}
  next
end

```

config web-proxy isolator-server

Parameter	Description	Type	Size	Default
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip
	Option	Description		
	<i>ip</i>	Use an IPv4 address for the forwarding proxy server.		
	<i>ipv6</i>	Use an IPv6 address for the forwarding proxy server.		
	<i>fqdn</i>	Use the FQDN for the forwarding proxy server.		
comment	Comment.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255							
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	sdwan						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description									
sdwan	Set outgoing interface by SD-WAN or policy routing rules.									
specify	Set outgoing interface manually.									
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified	0.0.0.0						
ipv6	Forward proxy server IPv6 address.	ipv6-address	Not Specified	::						
masquerade	Enable/disable use of the of the IP address of the outgoing interface as the client IP address (default = enable)	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of the IP address of the outgoing interface as the client IP address.</td></tr><tr><td>disable</td><td>Disable use of the of the IP address of the outgoing interface as the client IP address.</td></tr></table>				Option	Description	enable	Enable use of the IP address of the outgoing interface as the client IP address.	disable	Disable use of the of the IP address of the outgoing interface as the client IP address.
Option	Description									
enable	Enable use of the IP address of the outgoing interface as the client IP address.									
disable	Disable use of the of the IP address of the outgoing interface as the client IP address.									
name	Server name.	string	Maximum length: 63							
port	Port number that the forwarding server expects to receive HTTP sessions on (1 - 65535, default = 3128).	integer	Minimum value: 1 Maximum value: 65535	3128						
vrf-select	VRF ID used for connection to server.	integer	Minimum value: 0 Maximum value: 511	-1						

config web-proxy profile

Configure web proxy profiles.

```

config web-proxy profile
  Description: Configure web proxy profiles.
  edit <name>
    set header-client-ip [pass|add|...]
    set header-front-end-https [pass|add|...]
    set header-via-request [pass|add|...]
    set header-via-response [pass|add|...]
    set header-x-authenticated-groups [pass|add|...]
    set header-x-authenticated-user [pass|add|...]
    set header-x-forwarded-client-cert [pass|add|...]
    set header-x-forwarded-for [pass|add|...]
  config headers
    Description: Configure HTTP forwarded requests headers.
    edit <id>
      set action [add-to-request|add-to-response|...]
      set add-option [append|new-on-not-found|...]
      set base64-encoding [disable|enable]
      set content {string}
      set dstaddr <name1>, <name2>, ...
      set dstaddr6 <name1>, <name2>, ...
      set name {string}
      set protocol {option1}, {option2}, ...
    next
  end
  set log-header-change [enable|disable]
  set strip-encoding [enable|disable]
next
end

```

config web-proxy profile

Parameter	Description	Type	Size	Default								
header-client-ip	Action to take on the HTTP client-IP header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
	Option	Description										
	<i>pass</i>	Forward the same HTTP header.										
	<i>add</i>	Add the HTTP header.										
<i>remove</i>	Remove the HTTP header.											
header-front-end-https	Action to take on the HTTP front-end-HTTPS header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-via-response	Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-x-authenticated-groups	Action to take on the HTTP x-authenticated-groups header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-x-authenticated-user	Action to take on the HTTP x-authenticated-user header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.					
Option	Description											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-x-forwarded-client-cert	Action to take on the HTTP x-forwarded-client-cert header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-x-forwarded-for	Action to take on the HTTP x-forwarded-for header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
log-header-change	Enable/disable logging HTTP header changes.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Enable/disable logging HTTP header changes.</td></tr><tr><td><i>disable</i></td><td>Disable Enable/disable logging HTTP header changes.</td></tr></table>	Option	Description	<i>enable</i>	Enable Enable/disable logging HTTP header changes.	<i>disable</i>	Disable Enable/disable logging HTTP header changes.					
Option	Description											
<i>enable</i>	Enable Enable/disable logging HTTP header changes.											
<i>disable</i>	Disable Enable/disable logging HTTP header changes.											
name	Profile name.	string	Maximum length: 63									
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable stripping of unsupported encoding from the request header.</td></tr><tr><td><i>disable</i></td><td>Disable stripping of unsupported encoding from the request header.</td></tr></table>	Option	Description	<i>enable</i>	Enable stripping of unsupported encoding from the request header.	<i>disable</i>	Disable stripping of unsupported encoding from the request header.					
Option	Description											
<i>enable</i>	Enable stripping of unsupported encoding from the request header.											
<i>disable</i>	Disable stripping of unsupported encoding from the request header.											

config headers

Parameter	Description	Type	Size	Default														
action	Configure adding, removing, or logging of the HTTP header entry in HTTP requests and responses.	option	-	add-to-request														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>add-to-request</i></td><td>Add the HTTP header to request.</td></tr><tr><td><i>add-to-response</i></td><td>Add the HTTP header to response.</td></tr><tr><td><i>remove-from-request</i></td><td>Remove the HTTP header from request.</td></tr><tr><td><i>remove-from-response</i></td><td>Remove the HTTP header from response.</td></tr><tr><td><i>monitor-request</i></td><td>Record the HTTP header in utm-webfilter log.</td></tr><tr><td><i>monitor-response</i></td><td>Record the HTTP header in utm-webfilter log.</td></tr></table>	Option	Description	<i>add-to-request</i>	Add the HTTP header to request.	<i>add-to-response</i>	Add the HTTP header to response.	<i>remove-from-request</i>	Remove the HTTP header from request.	<i>remove-from-response</i>	Remove the HTTP header from response.	<i>monitor-request</i>	Record the HTTP header in utm-webfilter log.	<i>monitor-response</i>	Record the HTTP header in utm-webfilter log.			
Option	Description																	
<i>add-to-request</i>	Add the HTTP header to request.																	
<i>add-to-response</i>	Add the HTTP header to response.																	
<i>remove-from-request</i>	Remove the HTTP header from request.																	
<i>remove-from-response</i>	Remove the HTTP header from response.																	
<i>monitor-request</i>	Record the HTTP header in utm-webfilter log.																	
<i>monitor-response</i>	Record the HTTP header in utm-webfilter log.																	
add-option	Configure options to append content to existing HTTP header or add new HTTP header.	option	-	new														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>append</i></td><td>Append content to existing HTTP header or create new header if HTTP header is not found.</td></tr><tr><td><i>new-on-not-found</i></td><td>Create new header only if existing HTTP header is not found.</td></tr><tr><td><i>new</i></td><td>Create new header regardless if existing HTTP header is found or not.</td></tr><tr><td><i>replace</i></td><td>Replace content to existing HTTP header or create new header if HTTP header is not found.</td></tr><tr><td><i>replace-when-match</i></td><td>Replace content to existing HTTP header.</td></tr></table>	Option	Description	<i>append</i>	Append content to existing HTTP header or create new header if HTTP header is not found.	<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.	<i>new</i>	Create new header regardless if existing HTTP header is found or not.	<i>replace</i>	Replace content to existing HTTP header or create new header if HTTP header is not found.	<i>replace-when-match</i>	Replace content to existing HTTP header.					
Option	Description																	
<i>append</i>	Append content to existing HTTP header or create new header if HTTP header is not found.																	
<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.																	
<i>new</i>	Create new header regardless if existing HTTP header is found or not.																	
<i>replace</i>	Replace content to existing HTTP header or create new header if HTTP header is not found.																	
<i>replace-when-match</i>	Replace content to existing HTTP header.																	
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of base64 encoding of HTTP content.</td></tr><tr><td><i>enable</i></td><td>Enable use of base64 encoding of HTTP content.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of base64 encoding of HTTP content.	<i>enable</i>	Enable use of base64 encoding of HTTP content.											
Option	Description																	
<i>disable</i>	Disable use of base64 encoding of HTTP content.																	
<i>enable</i>	Enable use of base64 encoding of HTTP content.																	

Parameter	Description	Type	Size	Default						
content	HTTP header content.	string	Maximum length: 3999							
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79							
dstaddr6 <name>	Destination address and address group names (IPv6). Address name.	string	Maximum length: 79							
id	HTTP forwarded header id.	integer	Minimum value: 0 Maximum value: 4294967295							
name	HTTP forwarded header name.	string	Maximum length: 79							
protocol	Configure protocol(s) to take add-option action on (HTTP, HTTPS, or both).	option	-	https http						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>https</td><td>Perform add-option action on HTTPS.</td></tr><tr><td>http</td><td>Perform add-option action on HTTP.</td></tr></table>				Option	Description	https	Perform add-option action on HTTPS.	http	Perform add-option action on HTTP.
Option	Description									
https	Perform add-option action on HTTPS.									
http	Perform add-option action on HTTP.									

config web-proxy url-match

Exempt URLs from web proxy forwarding, caching and fast-fallback.

```

config web-proxy url-match
  Description: Exempt URLs from web proxy forwarding, caching and fast-fallback.
  edit <name>
    set cache-exemption [enable|disable]
    set comment {var-string}
    set fast-fallback {string}
    set forward-server {string}
    set status [enable|disable]
    set url-pattern {string}
  next
end

```

config web-proxy url-match

Parameter	Description	Type	Size	Default
cache-exemption	Enable/disable exempting this URL pattern from caching.	option	-	disable
	Option Description			
	<i>enable</i>	Enable exempting this URL pattern from caching.		
	<i>disable</i>	Disable exempting this URL pattern from caching.		
comment	Comment.	var-string	Maximum length: 255	
fast-fallback	Fast fallback configuration entry name.	string	Maximum length: 63	
forward-server	Forward server name.	string	Maximum length: 63	
name	Configure a name for the URL to be exempted.	string	Maximum length: 63	
status	Enable/disable exempting the URLs matching the URL pattern from web proxy forwarding, caching and fast-fallback.	option	-	enable
	Option Description			
	<i>enable</i>	Enable exempting the matching URLs.		
	<i>disable</i>	Disable exempting the matching URLs.		
url-pattern	URL pattern to be exempted from web proxy forwarding, caching and fast-fallback.	string	Maximum length: 511	

config web-proxy wisp

Configure Websense Integrated Services Protocol (WISP) servers.

```
config web-proxy wisp
  Description: Configure Websense Integrated Services Protocol (WISP) servers.
  edit <name>
    set comment {var-string}
    set max-connections {integer}
    set outgoing-ip {ipv4-address-any}
    set server-ip {ipv4-address-any}
    set server-port {integer}
    set timeout {integer}
```

```
next
end
```

config web-proxy wisp

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
max-connections	Maximum number of web proxy WISP connections (4 - 4096, default = 64).	integer	Minimum value: 4 Maximum value: 4096	64
name	Server name.	string	Maximum length: 35	
outgoing-ip	WISP outgoing IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-ip	WISP server IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-port	WISP server port (1 - 65535, default = 15868).	integer	Minimum value: 1 Maximum value: 65535	15868
timeout	Period of time before WISP requests time out (1 - 15 sec, default = 5).	integer	Minimum value: 1 Maximum value: 15	5

webfilter

This section includes syntax for the following commands:

- [config webfilter content-header on page 2379](#)
- [config webfilter content on page 2377](#)
- [config webfilter fortiguard on page 2380](#)
- [config webfilter ftgd-local-cat on page 2382](#)
- [config webfilter ftgd-local-rating on page 2383](#)
- [config webfilter ftgd-local-risk on page 2384](#)
- [config webfilter ftgd-risk-level on page 2385](#)
- [config webfilter ips-urlfilter-cache-setting on page 2385](#)
- [config webfilter ips-urlfilter-setting on page 2386](#)
- [config webfilter ips-urlfilter-setting6 on page 2387](#)
- [config webfilter override on page 2387](#)
- [config webfilter profile on page 2389](#)
- [config webfilter search-engine on page 2406](#)
- [config webfilter urlfilter on page 2408](#)

config webfilter content

Configure Web filter banned word table.

```
config webfilter content
  Description: Configure Web filter banned word table.
  edit <id>
    set comment {var-string}
    config entries
      Description: Configure banned word entries.
      edit <name>
        set action [block|exempt]
        set lang [western|simch|...]
        set pattern-type [wildcard|regex]
        set score {integer}
        set status [enable|disable]
      next
    end
    set name {string}
  next
end
```

config webfilter content

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default
action	Block or exempt word when a match is found.	option	-	block
	Option	Description		
	<i>block</i>	Block matches.		
	<i>exempt</i>	Exempt matches.		
lang	Language of banned word.	option	-	western
	Option	Description		
	<i>western</i>	Western.		
	<i>simch</i>	Simplified Chinese.		
	<i>trach</i>	Traditional Chinese.		
	<i>japanese</i>	Japanese.		
	<i>korean</i>	Korean.		
	<i>french</i>	French.		
	<i>thai</i>	Thai.		
	<i>spanish</i>	Spanish.		
	<i>cyrillic</i>	Cyrillic.		
name	Banned word.	string	Maximum length: 127	
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regex</i>	Perl regular expression.		
score	Score, to be applied every time the word appears on a web page (0 - 4294967295, default = 10).	integer	Minimum value: 10 0 Maximum value: 4294967295	
status	Enable/disable banned word.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config webfilter content-header

Configure content types used by Web filter.

```

config webfilter content-header
  Description: Configure content types used by Web filter.
  edit <id>
    set comment {var-string}
    config entries
      Description: Configure content types used by web filter.
      edit <pattern>
        set action [block|allow|...]
        set category {user}
      next
    end
    set name {string}
  next
end

```

config webfilter content-header

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default
action	Action to take for this content type.	option	-	allow
	Option	Description		
	block	Block content type.		
	allow	Allow content type.		
	exempt	Exempt content type.		
category	Categories that this content type applies to.	user	Not Specified	all
pattern	Content type (regular expression).	string	Maximum length: 31	

config webfilter fortiguard

Configure FortiGuard Web Filter service.

```

config webfilter fortiguard
    Description: Configure FortiGuard Web Filter service.
    set cache-mem-permille {integer}
    set cache-mode [ttl|db-ver]
    set cache-prefix-match [enable|disable]
    set close-ports [enable|disable]
    set embed-image [enable|disable]
    set ovr-auth-https [enable|disable]
    set ovr-auth-port-http {integer}
    set ovr-auth-port-https {integer}
    set ovr-auth-port-https-flow {integer}
    set ovr-auth-port-warning {integer}
    set request-packet-size-limit {integer}
    set warn-auth-https [enable|disable]
end

```

config webfilter fortiguard

Parameter	Description	Type	Size	Default						
cache-mem-permille	Maximum permille of available memory allocated to caching (1 - 150).	integer	Minimum value: 1 Maximum value: 150	1						
cache-mode	Cache entry expiration mode.	option	-	ttl						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ttl</td><td>Expire cache items by time-to-live.</td></tr><tr><td>db-ver</td><td>Expire cache items when the server DB version changes.</td></tr></table>	Option	Description	ttl	Expire cache items by time-to-live.	db-ver	Expire cache items when the server DB version changes.			
Option	Description									
ttl	Expire cache items by time-to-live.									
db-ver	Expire cache items when the server DB version changes.									
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
embed-image	Enable/disable embedding images into replacement messages (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									

Parameter	Description	Type	Size	Default
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication.	integer	Minimum value: 0 Maximum value: 65535	8008
ovrd-auth-port-https	Port to use for FortiGuard Web Filter HTTPS override authentication in proxy mode.	integer	Minimum value: 0 Maximum value: 65535	8010
ovrd-auth-port-https-flow	Port to use for FortiGuard Web Filter HTTPS override authentication in flow mode.	integer	Minimum value: 0 Maximum value: 65535	8015
ovrd-auth-port-warning	Port to use for FortiGuard Web Filter Warning override authentication.	integer	Minimum value: 0 Maximum value: 65535	8020
request-packet-size-limit	Limit size of URL request packets sent to FortiGuard server (0 for default).	integer	Minimum value: 576 Maximum value: 10000	0
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	

config webfilter ftgd-local-cat

Configure FortiGuard Web Filter local categories.

```
config webfilter ftgd-local-cat
    Description: Configure FortiGuard Web Filter local categories.
    edit <desc>
        set id {integer}
        set status [enable|disable]
```

```
next
end
```

config webfilter ftgd-local-cat

Parameter	Description	Type	Size	Default
desc	Local category description.	string	Maximum length: 79	
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0
status	Enable/disable the local category.	option	-	enable
		Option	Description	
		enable	Enable the local category.	
		disable	Disable the local category.	

config webfilter ftgd-local-rating

Configure local FortiGuard Web Filter local ratings.

```
config webfilter ftgd-local-rating
  Description: Configure local FortiGuard Web Filter local ratings.
  edit <url>
    set comment {var-string}
    set rating {user}
    set status [enable|disable]
  next
end
```

config webfilter ftgd-local-rating

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
rating	Local rating.	user	Not Specified	
status	Enable/disable local rating.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local rating.		
	<i>disable</i>	Disable local rating.		
url	URL to rate locally.	string	Maximum length: 511	

config webfilter ftgd-local-risk

Configure FortiGuard Web Filter local risk score.

```
config webfilter ftgd-local-risk
  Description: Configure FortiGuard Web Filter local risk score.
  edit <url>
    set comment {var-string}
    set risk-score {integer}
    set status [enable|disable]
  next
end
```

config webfilter ftgd-local-risk

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
risk-score	Local risk score.	integer	Minimum value: 0 Maximum value: 100	0
status	Enable/disable local risk score.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local risk level.		
	<i>disable</i>	Disable local risk level.		
url	URL to rate locally.	string	Maximum length: 511	

config webfilter ftgd-risk-level

Configure FortiGuard Web Filter risk level.

```
config webfilter ftgd-risk-level
  Description: Configure FortiGuard Web Filter risk level.
  edit <name>
    set high {integer}
    set low {integer}
  next
end
```

config webfilter ftgd-risk-level

Parameter	Description	Type	Size	Default
high	Risk level high.	integer	Minimum value: 0 Maximum value: 100	0
low	Risk level low.	integer	Minimum value: 0 Maximum value: 100	0
name	Risk level name.	string	Maximum length: 35	

config webfilter ips-urlfilter-cache-setting

Configure IPS URL filter cache settings.

```
config webfilter ips-urlfilter-cache-setting
  Description: Configure IPS URL filter cache settings.
  set dns-retry-interval {integer}
  set extended-ttl {integer}
end
```

config webfilter ips-urlfilter-cache-setting

Parameter	Description	Type	Size	Default
dns-retry-interval	Retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. 0 means use DNS server's TTL only.	integer	Minimum value: 0 Maximum value: 2147483	0
extended-ttl	Extend time to live beyond reported by DNS. Use of 0 means use DNS server's TTL.	integer	Minimum value: 0 Maximum value: 2147483	0

config webfilter ips-urlfilter-setting

Configure IPS URL filter settings.

```
config webfilter ips-urlfilter-setting
  Description: Configure IPS URL filter settings.
  set device {string}
  set distance {integer}
  set gateway {ipv4-address}
  set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance (1 - 255) for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway	Gateway IP address for this route.	ipv4-address	Not Specified	0.0.0.0
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IP address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter ips-urlfilter-setting6

Configure IPS URL filter settings for IPv6.

```
config webfilter ips-urlfilter-setting6
  Description: Configure IPS URL filter settings for IPv6.
  set device {string}
  set distance {integer}
  set gateway6 {ipv6-address}
  set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting6

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance (1 - 255) for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway6	Gateway IPv6 address for this route.	ipv6-address	Not Specified	::
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IPv6 address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter override

Configure FortiGuard Web Filter administrative overrides.

```
config webfilter override
  Description: Configure FortiGuard Web Filter administrative overrides.
  edit <id>
    set expires {user}
    set initiator {string}
    set ip {ipv4-address}
    set ip6 {ipv6-address}
    set new-profile {string}
    set old-profile {string}
    set scope [user|user-group|...]
    set status [enable|disable]
    set user {string}
    set user-group {string}
  end
```

next
end

config webfilter override

Parameter	Description	Type	Size	Default
expires	Override expiration date and time, from 5 minutes to 365 from now (format: yyyy/mm/dd hh:mm:ss).	user	Not Specified	1969/12/31 16:00:00 **
id	Override rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
initiator	Initiating user of override (read-only setting).	string	Maximum length: 64	
ip	IPv4 address which the override applies.	ipv4-address	Not Specified	0.0.0.0
ip6	IPv6 address which the override applies.	ipv6-address	Not Specified	::
new-profile	Name of the new web filter profile used by the override.	string	Maximum length: 47	
old-profile	Name of the web filter profile which the override applies.	string	Maximum length: 47	
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.	option	-	user
	Option Description			
	user	Override the specified user.		
	user-group	Override the specified user group.		
	ip	Override the specified IP address.		
	ip6	Override the specified IPv6 address.		
status	Enable/disable override rule.	option	-	disable
	Option Description			
	enable	Enable override rule.		
	disable	Disable override rule.		
user	Name of the user which the override applies.	string	Maximum length: 64	

Parameter	Description	Type	Size	Default
user-group	Specify the user group for which the override applies.	string	Maximum length: 63	

** Values may differ between models.

config webfilter profile

Configure Web filter profiles.

```

config webfilter profile
  Description: Configure Web filter profiles.
  edit <name>
    config antiphish
      Description: AntiPhishing profile.
      set authentication [domain-controller|ldap]
      set check-basic-auth [enable|disable]
      set check-uri [enable|disable]
      set check-username-only [enable|disable]
    config custom-patterns
      Description: Custom username and password regex patterns.
      edit <pattern>
        set category [username|password]
        set type [regex|literal]
      next
    end
    set default-action [exempt|log|...]
    set domain-controller {string}
    config inspection-entries
      Description: AntiPhishing entries.
      edit <name>
        set action [exempt|log|...]
        set fortiguard-category {user}
      next
    end
    set ldap {string}
    set max-body-len {integer}
    set status [enable|disable]
  end
  set comment {var-string}
  set extended-log [enable|disable]
  set feature-set [flow|proxy]
  config ftgd-wf
    Description: FortiGuard Web Filter settings.
    set exempt-quota {user}
    config filters
      Description: FortiGuard filters.
      edit <id>
        set action [block|authenticate|...]

```

```

        set auth-usr-grp <name1>, <name2>, ...
        set category {integer}
        set log [enable|disable]
        set override-replacemsg {string}
        set warn-duration {user}
        set warning-duration-type [session|timeout]
        set warning-prompt [per-domain|per-category]
    next
end
set max-quota-timeout {integer}
set options {option1}, {option2}, ...
set ovrd {user}
config quota
    Description: FortiGuard traffic quota settings.
    edit <id>
        set category {user}
        set duration {user}
        set override-replacemsg {string}
        set type [time|traffic]
        set unit [B|KB|...]
        set value {integer}
    next
end
set rate-crl-urls [disable|enable]
set rate-css-urls [disable|enable]
set rate-javascript-urls [disable|enable]
config risk
    Description: FortiGuard risk level settings.
    edit <id>
        set action [block|monitor]
        set log [enable|disable]
        set risk-level {string}
    next
end
end
set https-replacemsg [enable|disable]
set log-all-url [enable|disable]
set options {option1}, {option2}, ...
config override
    Description: Web Filter override settings.
    set ovrd-cookie [allow|deny]
    set ovrd-dur {user}
    set ovrd-dur-mode [constant|ask]
    set ovrd-scope [user|user-group|...]
    set ovrd-user-group <name1>, <name2>, ...
    set profile <name1>, <name2>, ...
    set profile-attribute [User-Name|NAS-IP-Address|...]
    set profile-type [list|radius]
end
set ovrd-perm {option1}, {option2}, ...
set post-action [normal|block]
set replacemsg-group {string}

```

```

config web
    Description: Web content filtering settings.
    set allowlist {option1}, {option2}, ...
    set blacklist [enable|disable]
    set bword-table {integer}
    set bword-threshold {integer}
    set content-header-list {integer}
    set keyword-match <pattern1>, <pattern2>, ...
    set log-search [enable|disable]
    set safe-search {option1}, {option2}, ...
    set urlfilter-table {integer}
    set vimeo-restrict {string}
    set youtube-restrict [none|strict|...]
end
set web-antiphishing-log [enable|disable]
set web-content-log [enable|disable]
set web-extended-all-action-log [enable|disable]
set web-filter-activex-log [enable|disable]
set web-filter-applet-log [enable|disable]
set web-filter-command-block-log [enable|disable]
set web-filter-cookie-log [enable|disable]
set web-filter-cookie-removal-log [enable|disable]
set web-filter-js-log [enable|disable]
set web-filter-jscript-log [enable|disable]
set web-filter-referer-log [enable|disable]
set web-filter-unknown-log [enable|disable]
set web-filter-vbs-log [enable|disable]
set web-flow-log-encoding [utf-8|punycode]
set web-ftgd-err-log [enable|disable]
set web-ftgd-quota-usage [enable|disable]
set web-invalid-domain-log [enable|disable]
set web-url-log [enable|disable]
set wisp [enable|disable]
set wisp-algorithm [primary-secondary|round-robin|...]
set wisp-servers <name1>, <name2>, ...
next
end

```

config webfilter profile

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
extended-log	Enable/disable extended logging for web filtering.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable setting.		
feature-set	Flow/proxy feature set.	option	-	flow
	Option	Description		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
https-replacemsg	Enable replacement messages for HTTPS.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
log-all-url	Enable/disable logging all URLs visited.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
name	Profile name.	string	Maximum length: 47	
options	Options.	option	-	
	Option	Description		
	<i>activexfilter</i>	ActiveX filter.		
	<i>cookiefilter</i>	Cookie filter.		
	<i>javafilter</i>	Java applet filter.		
	<i>block-invalid-url</i>	Block sessions contained an invalid domain name.		
	<i>jscript</i>	Javascript block.		
	<i>js</i>	JS block.		
	<i>vbs</i>	VB script block.		
	<i>unknown</i>	Unknown script block.		
	<i>intrinsic</i>	Intrinsic script block.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wf-referer</i></td><td>Referring block.</td></tr><tr><td><i>wf-cookie</i></td><td>Cookie block.</td></tr><tr><td><i>per-user-bal</i></td><td>Per-user block/allow list filter</td></tr></table>	Option	Description	<i>wf-referer</i>	Referring block.	<i>wf-cookie</i>	Cookie block.	<i>per-user-bal</i>	Per-user block/allow list filter					
	Option	Description												
	<i>wf-referer</i>	Referring block.												
	<i>wf-cookie</i>	Cookie block.												
<i>per-user-bal</i>	Per-user block/allow list filter													
ovrd-perm	Permitted override types.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bannedword-override</i></td><td>Banned word override.</td></tr><tr><td><i>urlfilter-override</i></td><td>URL filter override.</td></tr><tr><td><i>fortiguard-wf-override</i></td><td>FortiGuard Web Filter override.</td></tr><tr><td><i>contenttype-check-override</i></td><td>Content-type header override.</td></tr></table>	Option	Description	<i>bannedword-override</i>	Banned word override.	<i>urlfilter-override</i>	URL filter override.	<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.	<i>contenttype-check-override</i>	Content-type header override.			
	Option	Description												
	<i>bannedword-override</i>	Banned word override.												
	<i>urlfilter-override</i>	URL filter override.												
	<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.												
<i>contenttype-check-override</i>	Content-type header override.													
post-action	Action taken for HTTP POST traffic.	option	-	normal										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Normal, POST requests are allowed.</td></tr><tr><td><i>block</i></td><td>POST requests are blocked.</td></tr></table>	Option	Description	<i>normal</i>	Normal, POST requests are allowed.	<i>block</i>	POST requests are blocked.							
	Option	Description												
	<i>normal</i>	Normal, POST requests are allowed.												
<i>block</i>	POST requests are blocked.													
replacemsg-group	Replacement message group.	string	Maximum length: 35											
web-antiphishing-log	Enable/disable logging of AntiPhishing checks.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
web-content-log	Enable/disable logging logging blocked web content.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
web-extended-all-action-log	Enable/disable extended any filter action logging for web filtering.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-activex-log	Enable/disable logging ActiveX.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-applet-log	Enable/disable logging Java applets.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-command-block-log	Enable/disable logging blocked commands.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-cookie-log	Enable/disable logging cookie filtering.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-cookie-removal-log	Enable/disable logging blocked cookies.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
web-filter-js-log	Enable/disable logging Java scripts.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-jscript-log	Enable/disable logging JScripts.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-referer-log	Enable/disable logging referrers.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-unknown-log	Enable/disable logging unknown scripts.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-vbs-log	Enable/disable logging VBS scripts.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-flow-log-encoding	Log encoding in flow mode.	option	-	utf-8						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>utf-8</i></td><td>UTF-8 encoding.</td></tr><tr><td><i>punycode</i></td><td>Punycode encoding.</td></tr></table>	Option	Description	<i>utf-8</i>	UTF-8 encoding.	<i>punycode</i>	Punycode encoding.			
Option	Description									
<i>utf-8</i>	UTF-8 encoding.									
<i>punycode</i>	Punycode encoding.									

Parameter	Description	Type	Size	Default								
web-ftgd-err-log	Enable/disable logging rating errors.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
web-url-log	Enable/disable logging URL filtering.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
wisp	Enable/disable web proxy WISP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable web proxy WISP.</td></tr><tr><td><i>disable</i></td><td>Disable web proxy WISP.</td></tr></table>	Option	Description	<i>enable</i>	Enable web proxy WISP.	<i>disable</i>	Disable web proxy WISP.					
Option	Description											
<i>enable</i>	Enable web proxy WISP.											
<i>disable</i>	Disable web proxy WISP.											
wisp-algorithm	WISP server selection algorithm.	option	-	auto-learning								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>primary-secondary</i></td><td>Select the first healthy server in order.</td></tr><tr><td><i>round-robin</i></td><td>Select the next healthy server.</td></tr><tr><td><i>auto-learning</i></td><td>Select the lightest loading healthy server.</td></tr></table>	Option	Description	<i>primary-secondary</i>	Select the first healthy server in order.	<i>round-robin</i>	Select the next healthy server.	<i>auto-learning</i>	Select the lightest loading healthy server.			
Option	Description											
<i>primary-secondary</i>	Select the first healthy server in order.											
<i>round-robin</i>	Select the next healthy server.											
<i>auto-learning</i>	Select the lightest loading healthy server.											

Parameter	Description	Type	Size	Default
wisp-servers <name>	WISP servers. Server name.	string	Maximum length: 79	

config antiphish

Parameter	Description	Type	Size	Default						
authentication	Authentication methods.	option	-	domain-controller						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>domain-controller</i></td><td>Domain Controller to verify user credential.</td></tr><tr><td><i>ldap</i></td><td>LDAP to verify user credential.</td></tr></table>	Option	Description	<i>domain-controller</i>	Domain Controller to verify user credential.	<i>ldap</i>	LDAP to verify user credential.			
Option	Description									
<i>domain-controller</i>	Domain Controller to verify user credential.									
<i>ldap</i>	LDAP to verify user credential.									
check-basic-auth	Enable/disable checking of HTTP Basic Auth field for known credentials.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable checking of HTTP Basic Auth field for known credentials.</td></tr><tr><td><i>disable</i></td><td>Disable checking of HTTP Basic Auth field for known credentials.</td></tr></table>	Option	Description	<i>enable</i>	Enable checking of HTTP Basic Auth field for known credentials.	<i>disable</i>	Disable checking of HTTP Basic Auth field for known credentials.			
Option	Description									
<i>enable</i>	Enable checking of HTTP Basic Auth field for known credentials.									
<i>disable</i>	Disable checking of HTTP Basic Auth field for known credentials.									
check-uri	Enable/disable checking of GET URI parameters for known credentials.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable checking of GET URI for username and password fields.</td></tr><tr><td><i>disable</i></td><td>Disable checking of GET URI for username and password fields.</td></tr></table>	Option	Description	<i>enable</i>	Enable checking of GET URI for username and password fields.	<i>disable</i>	Disable checking of GET URI for username and password fields.			
Option	Description									
<i>enable</i>	Enable checking of GET URI for username and password fields.									
<i>disable</i>	Disable checking of GET URI for username and password fields.									
check-username-only	Enable/disable username only matching of credentials. Action will be taken for valid usernames regardless of password validity.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable username only credential matches.</td></tr><tr><td><i>disable</i></td><td>Disable username only credential matches.</td></tr></table>	Option	Description	<i>enable</i>	Enable username only credential matches.	<i>disable</i>	Disable username only credential matches.			
Option	Description									
<i>enable</i>	Enable username only credential matches.									
<i>disable</i>	Disable username only credential matches.									
default-action	Action to be taken when there is no matching rule.	option	-	exempt						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exempt</i></td><td>Exempt requests from matching.</td></tr></table>	Option	Description	<i>exempt</i>	Exempt requests from matching.					
Option	Description									
<i>exempt</i>	Exempt requests from matching.									

Parameter	Description	Type	Size	Default
	Option Description			
	<i>log</i>	Log all matched requests.		
	<i>block</i>	Block all matched requests.		
domain-controller	Domain for which to verify received credentials against.	string	Maximum length: 63	
ldap	LDAP server for which to verify received credentials against.	string	Maximum length: 63	
max-body-len	Maximum size of a POST body to check for credentials.	integer	Minimum value: 0 Maximum value: 4294967295	1024
status	Toggle AntiPhishing functionality.	option	-	disable
	Option Description			
	<i>enable</i>	Enable AntiPhishing functionality.		
	<i>disable</i>	Disable AntiPhishing functionality.		

config custom-patterns

Parameter	Description	Type	Size	Default
category	Category that the pattern matches.	option	-	username
	Option Description			
	<i>username</i>	Pattern matches username fields.		
	<i>password</i>	Pattern matches password fields.		
pattern	Target pattern.	string	Maximum length: 255	
type	Pattern will be treated either as a regex pattern or literal string.	option	-	regex
	Option Description			
	<i>regex</i>	Pattern will be treated as a regex pattern.		
	<i>literal</i>	Pattern will be treated as a literal string.		

config inspection-entries

Parameter	Description	Type	Size	Default
action	Action to be taken upon an AntiPhishing match.	option	-	exempt
	Option	Description		
	<i>exempt</i>	Exempt requests from matching.		
	<i>log</i>	Log all matched requests.		
	<i>block</i>	Block all matched requests.		
fortiguard-category	FortiGuard category to match.	user	Not Specified	0
name	Inspection target name.	string	Maximum length: 63	

config ftgd-wf

Parameter	Description	Type	Size	Default
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400	300
options	Options for FortiGuard Web Filter.	option	-	ftgd-disable
	Option	Description		
	<i>error-allow</i>	Allow web pages with a rating error to pass through.		
	<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.		
	<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.		
	<i>ftgd-disable</i>	Disable FortiGuard scanning.		
ovrd	Allow web filter profile overrides.	user	Not Specified	
rate-crl-urls	Enable/disable rating CRL by URL.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable rating CRL by URL.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable rating CRL by URL.		
rate-css-urls	Enable/disable rating CSS by URL.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable rating CSS by URL.		
	<i>enable</i>	Enable rating CSS by URL.		
rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable rating JavaScript by URL.		
	<i>enable</i>	Enable rating JavaScript by URL.		

config filters

Parameter	Description	Type	Size	Default
action	Action to take for matches.	option	-	monitor
	Option	Description		
	<i>block</i>	Block access.		
	<i>authenticate</i>	Authenticate user before allowing access.		
	<i>monitor</i>	Allow access while logging the action.		
	<i>warning</i>	Allow access after warning the user.		
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79	
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0
log	Enable/disable logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
override-replacemsg	Override replacement message.	string	Maximum length: 28	
warn-duration	Duration of warnings.	user	Not Specified	5m
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-	timeout
	Option	Description		
	<i>session</i>	After session ends.		
	<i>timeout</i>	After timeout occurs.		
warning-prompt	Warning prompts in each category or each domain.	option	-	per-category
	Option	Description		
	<i>per-domain</i>	Per-domain warnings.		
	<i>per-category</i>	Per-category warnings.		

config quota

Parameter	Description	Type	Size	Default
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	
duration	Duration of quota.	user	Not Specified	5m
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295	0
override-replacemsg	Override replacement message.	string	Maximum length: 28	
type	Quota type.	option	-	time
	Option	Description		
	<i>time</i>	Use a time-based quota.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>traffic</i></td><td>Use a traffic-based quota.</td></tr></table>				Option	Description	<i>traffic</i>	Use a traffic-based quota.						
	Option	Description												
<i>traffic</i>	Use a traffic-based quota.													
unit	Traffic quota unit of measurement.	option	-	MB										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>B</i></td><td>Quota in bytes.</td></tr><tr><td><i>KB</i></td><td>Quota in kilobytes.</td></tr><tr><td><i>MB</i></td><td>Quota in megabytes.</td></tr><tr><td><i>GB</i></td><td>Quota in gigabytes.</td></tr></table>				Option	Description	<i>B</i>	Quota in bytes.	<i>KB</i>	Quota in kilobytes.	<i>MB</i>	Quota in megabytes.	<i>GB</i>	Quota in gigabytes.
	Option	Description												
	<i>B</i>	Quota in bytes.												
	<i>KB</i>	Quota in kilobytes.												
	<i>MB</i>	Quota in megabytes.												
<i>GB</i>	Quota in gigabytes.													
value	Traffic quota value.	integer	Minimum value: 1024 1 Maximum value: 4294967295											

config risk

Parameter	Description	Type	Size	Default						
action	Action to take for matches.	option	-	monitor						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block access.</td></tr><tr><td><i>monitor</i></td><td>Allow access while logging the action.</td></tr></table>				Option	Description	<i>block</i>	Block access.	<i>monitor</i>	Allow access while logging the action.
	Option	Description								
	<i>block</i>	Block access.								
<i>monitor</i>	Allow access while logging the action.									
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0						
log	Enable/disable logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
risk-level	Risk level to be examined.	string	Maximum length: 35							

config override

Parameter	Description	Type	Size	Default												
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-	deny												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow browser-based (cookie) override.</td></tr><tr><td><i>deny</i></td><td>Deny browser-based (cookie) override.</td></tr></table>	Option	Description	<i>allow</i>	Allow browser-based (cookie) override.	<i>deny</i>	Deny browser-based (cookie) override.									
Option	Description															
<i>allow</i>	Allow browser-based (cookie) override.															
<i>deny</i>	Deny browser-based (cookie) override.															
ovrd-dur	Override duration.	user	Not Specified	15m												
ovrd-dur-mode	Override duration mode.	option	-	constant												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>constant</i></td><td>Constant mode.</td></tr><tr><td><i>ask</i></td><td>Prompt for duration when initiating an override.</td></tr></table>	Option	Description	<i>constant</i>	Constant mode.	<i>ask</i>	Prompt for duration when initiating an override.									
Option	Description															
<i>constant</i>	Constant mode.															
<i>ask</i>	Prompt for duration when initiating an override.															
ovrd-scope	Override scope.	option	-	user												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Override for the user.</td></tr><tr><td><i>user-group</i></td><td>Override for the user's group.</td></tr><tr><td><i>ip</i></td><td>Override for the initiating IP.</td></tr><tr><td><i>browser</i></td><td>Create browser-based (cookie) override.</td></tr><tr><td><i>ask</i></td><td>Prompt for scope when initiating an override.</td></tr></table>	Option	Description	<i>user</i>	Override for the user.	<i>user-group</i>	Override for the user's group.	<i>ip</i>	Override for the initiating IP.	<i>browser</i>	Create browser-based (cookie) override.	<i>ask</i>	Prompt for scope when initiating an override.			
Option	Description															
<i>user</i>	Override for the user.															
<i>user-group</i>	Override for the user's group.															
<i>ip</i>	Override for the initiating IP.															
<i>browser</i>	Create browser-based (cookie) override.															
<i>ask</i>	Prompt for scope when initiating an override.															
ovrd-user-group <name>	User groups with permission to use the override. User group name.	string	Maximum length: 79													
profile <name>	Web filter profile with permission to create overrides. Web profile.	string	Maximum length: 79													
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-	Login-LAT-Service												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>User-Name</i></td><td>Use this attribute.</td></tr><tr><td><i>NAS-IP-Address</i></td><td>Use this attribute.</td></tr></table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.									
Option	Description															
<i>User-Name</i>	Use this attribute.															
<i>NAS-IP-Address</i>	Use this attribute.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>Framed-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Netmask</i>	Use this attribute.		
	<i>Filter-Id</i>	Use this attribute.		
	<i>Login-IP-Host</i>	Use this attribute.		
	<i>Reply-Message</i>	Use this attribute.		
	<i>Callback-Number</i>	Use this attribute.		
	<i>Callback-Id</i>	Use this attribute.		
	<i>Framed-Route</i>	Use this attribute.		
	<i>Framed-IPX-Network</i>	Use this attribute.		
	<i>Class</i>	Use this attribute.		
	<i>Called-Station-Id</i>	Use this attribute.		
	<i>Calling-Station-Id</i>	Use this attribute.		
	<i>NAS-Identifier</i>	Use this attribute.		
	<i>Proxy-State</i>	Use this attribute.		
	<i>Login-LAT-Service</i>	Use this attribute.		
	<i>Login-LAT-Node</i>	Use this attribute.		
	<i>Login-LAT-Group</i>	Use this attribute.		
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.		
	<i>Acct-Session-Id</i>	Use this attribute.		
<i>Acct-Multi-Session-Id</i>	Use this attribute.			
profile-type	Override profile type.	option	-	list

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>list</i>	Profile chosen from list.		
	<i>radius</i>	Profile determined by RADIUS server.		

config web

Parameter	Description	Type	Size	Default
allowlist	FortiGuard allowlist settings.	option	-	
	Option	Description		
	<i>exempt-av</i>	Exempt antivirus.		
	<i>exempt-webcontent</i>	Exempt web content.		
	<i>exempt-activex-java-cookie</i>	Exempt ActiveX-JAVA-Cookie.		
	<i>exempt-dlp</i>	Exempt DLP.		
	<i>exempt-rangeblock</i>	Exempt RangeBlock.		
	<i>extended-log-others</i>	Support extended log.		
blocklist	Enable/disable automatic addition of URLs detected by FortiSandbox to blocklist.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bword-table	Banned word table ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	
bword-threshold	Banned word score threshold.	integer	Minimum value: 10 0 Maximum value: 2147483647	

Parameter	Description	Type	Size	Default								
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295	0								
keyword-match <pattern>	Search keywords to log when match is found. Pattern/keyword to search for.	string	Maximum length: 79	**								
log-search	Enable/disable logging all search phrases.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
safe-search	Safe search type.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>url</i></td><td>Insert safe search string into URL.</td></tr><tr><td><i>header</i></td><td>Insert safe search header.</td></tr></table>	Option	Description	<i>url</i>	Insert safe search string into URL.	<i>header</i>	Insert safe search header.					
Option	Description											
<i>url</i>	Insert safe search string into URL.											
<i>header</i>	Insert safe search header.											
urlfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
vimeo-restrict	Set Vimeo-restrict ("7" = don't show mature content, "134" = don't show unrated and mature content). A value of cookie "content_rating".	string	Maximum length: 63									
youtube-restrict	YouTube EDU filter level.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Full access for YouTube.</td></tr><tr><td><i>strict</i></td><td>Strict access for YouTube.</td></tr><tr><td><i>moderate</i></td><td>Moderate access for YouTube.</td></tr></table>	Option	Description	<i>none</i>	Full access for YouTube.	<i>strict</i>	Strict access for YouTube.	<i>moderate</i>	Moderate access for YouTube.			
Option	Description											
<i>none</i>	Full access for YouTube.											
<i>strict</i>	Strict access for YouTube.											
<i>moderate</i>	Moderate access for YouTube.											

config webfilter search-engine

Configure web filter search engines.

```
config webfilter search-engine
    Description: Configure web filter search engines.
```

```

edit <name>
    set charset [utf-8|gb2312]
    set hostname {string}
    set query {string}
    set safesearch [disable|url|...]
    set safesearch-str {string}
    set url {string}
next
end

```

config webfilter search-engine

Parameter	Description	Type	Size	Default																		
charset	Search engine charset.	option	-	utf-8																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>utf-8</td><td>UTF-8 encoding.</td></tr><tr><td>gb2312</td><td>GB2312 encoding.</td></tr></table>				Option	Description	utf-8	UTF-8 encoding.	gb2312	GB2312 encoding.												
	Option	Description																				
	utf-8	UTF-8 encoding.																				
gb2312	GB2312 encoding.																					
hostname	Hostname (regular expression).	string	Maximum length: 127																			
name	Search engine name.	string	Maximum length: 35																			
query	Code used to prefix a query (must end with an equals character).	string	Maximum length: 15																			
safesearch	Safe search method. You can disable safe search, add the safe search string to URLs, or insert a safe search header.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Site does not support safe search.</td></tr><tr><td>url</td><td>Safe search selected with a parameter in the URL.</td></tr><tr><td>header</td><td>Safe search selected by search header (i.e. youtube.edu).</td></tr><tr><td>translate</td><td>Perform URL FortiGuard check on translated URL.</td></tr><tr><td>yt-pattern</td><td>Pattern to match YouTube channel ID.</td></tr><tr><td>yt-scan</td><td>Perform IPS scan.</td></tr><tr><td>yt-video</td><td>Pattern to match YouTube video name.</td></tr><tr><td>yt-channel</td><td>Pattern to match YouTube channel name.</td></tr></table>				Option	Description	disable	Site does not support safe search.	url	Safe search selected with a parameter in the URL.	header	Safe search selected by search header (i.e. youtube.edu).	translate	Perform URL FortiGuard check on translated URL.	yt-pattern	Pattern to match YouTube channel ID.	yt-scan	Perform IPS scan.	yt-video	Pattern to match YouTube video name.	yt-channel	Pattern to match YouTube channel name.
	Option	Description																				
	disable	Site does not support safe search.																				
	url	Safe search selected with a parameter in the URL.																				
	header	Safe search selected by search header (i.e. youtube.edu).																				
	translate	Perform URL FortiGuard check on translated URL.																				
	yt-pattern	Pattern to match YouTube channel ID.																				
	yt-scan	Perform IPS scan.																				
yt-video	Pattern to match YouTube video name.																					
yt-channel	Pattern to match YouTube channel name.																					

Parameter	Description	Type	Size	Default
safesearch-str	Safe search parameter used in the URL in URL mode. In translate mode, it provides either the regex to translate the URL or the special case to translate the URL.	string	Maximum length: 255	
url	URL (regular expression).	string	Maximum length: 127	

config webfilter urlfilter

Configure URL filter lists.

```

config webfilter urlfilter
  Description: Configure URL filter lists.
  edit <id>
    set comment {var-string}
    config entries
      Description: URL filter entries.
      edit <id>
        set action [exempt|block|...]
        set antiphish-action [block|log]
        set dns-address-family [ipv4|ipv6|...]
        set exempt {option1}, {option2}, ...
        set referrer-host {string}
        set status [enable|disable]
        set type [simple|regex|...]
        set url {string}
        set web-proxy-profile {string}
      next
    end
    set include-subdomains [enable|disable]
    set ip-addr-block [enable|disable]
    set ip4-mapped-ip6 [enable|disable]
    set name {string}
    set one-arm-ips-urlfilter [enable|disable]
  next
end

```

config webfilter urlfilter

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 0 Maximum value: 4294967295	0						
include-subdomains	Enable/disable matching subdomains. Applies only to simple type (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable matching subdomains. Applies only to simple type.</td></tr><tr><td>disable</td><td>Disable matching subdomains. Applies only to simple type.</td></tr></table>	Option	Description	enable	Enable matching subdomains. Applies only to simple type.	disable	Disable matching subdomains. Applies only to simple type.			
Option	Description									
enable	Enable matching subdomains. Applies only to simple type.									
disable	Disable matching subdomains. Applies only to simple type.									
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable blocking URLs when the hostname appears as an IP address.</td></tr><tr><td>disable</td><td>Disable blocking URLs when the hostname appears as an IP address.</td></tr></table>	Option	Description	enable	Enable blocking URLs when the hostname appears as an IP address.	disable	Disable blocking URLs when the hostname appears as an IP address.			
Option	Description									
enable	Enable blocking URLs when the hostname appears as an IP address.									
disable	Disable blocking URLs when the hostname appears as an IP address.									
ip4-mapped-ip6	Enable/disable matching of IPv4 mapped IPv6 URLs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable matching IPv4 mapped IPv6 URLs.</td></tr><tr><td>disable</td><td>Disable matching IPv4 mapped IPv6 URLs.</td></tr></table>	Option	Description	enable	Enable matching IPv4 mapped IPv6 URLs.	disable	Disable matching IPv4 mapped IPv6 URLs.			
Option	Description									
enable	Enable matching IPv4 mapped IPv6 URLs.									
disable	Disable matching IPv4 mapped IPv6 URLs.									
name	Name of URL filter list.	string	Maximum length: 63							
one-arm-ips-urlfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DNS resolver for one-arm IPS URL filter operation.</td></tr><tr><td>disable</td><td>Disable DNS resolver for one-arm IPS URL filter operation.</td></tr></table>	Option	Description	enable	Enable DNS resolver for one-arm IPS URL filter operation.	disable	Disable DNS resolver for one-arm IPS URL filter operation.			
Option	Description									
enable	Enable DNS resolver for one-arm IPS URL filter operation.									
disable	Disable DNS resolver for one-arm IPS URL filter operation.									

config entries

Parameter	Description	Type	Size	Default
action	Action to take for URL filter matches.	option	-	exempt

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exempt</i></td><td>Exempt matches.</td></tr><tr><td><i>block</i></td><td>Block matches.</td></tr><tr><td><i>allow</i></td><td>Allow matches (no log).</td></tr><tr><td><i>monitor</i></td><td>Allow matches (with log).</td></tr></table>	Option	Description	<i>exempt</i>	Exempt matches.	<i>block</i>	Block matches.	<i>allow</i>	Allow matches (no log).	<i>monitor</i>	Allow matches (with log).							
	Option	Description																
	<i>exempt</i>	Exempt matches.																
	<i>block</i>	Block matches.																
	<i>allow</i>	Allow matches (no log).																
<i>monitor</i>	Allow matches (with log).																	
antiphish-action	Action to take for AntiPhishing matches.	option	-	block														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block matches.</td></tr><tr><td><i>log</i></td><td>Allow matches with log.</td></tr></table>	Option	Description	<i>block</i>	Block matches.	<i>log</i>	Allow matches with log.											
	Option	Description																
	<i>block</i>	Block matches.																
<i>log</i>	Allow matches with log.																	
dns-address-family	Resolve IPv4 address, IPv6 address, or both from DNS server.	option	-	ipv4														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>Resolve IPv4 address from DNS server.</td></tr><tr><td><i>ipv6</i></td><td>Resolve IPv6 address from DNS server.</td></tr><tr><td><i>both</i></td><td>Resolve both IPv4 and IPv6 addresses from DNS server.</td></tr></table>	Option	Description	<i>ipv4</i>	Resolve IPv4 address from DNS server.	<i>ipv6</i>	Resolve IPv6 address from DNS server.	<i>both</i>	Resolve both IPv4 and IPv6 addresses from DNS server.									
	Option	Description																
	<i>ipv4</i>	Resolve IPv4 address from DNS server.																
	<i>ipv6</i>	Resolve IPv6 address from DNS server.																
<i>both</i>	Resolve both IPv4 and IPv6 addresses from DNS server.																	
exempt	If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple options with a space.	option	-	av web-content activex-java-cookie dlp fortiguard range-block antiphish all														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>av</i></td><td>AntiVirus scanning.</td></tr><tr><td><i>web-content</i></td><td>Web filter content matching.</td></tr><tr><td><i>activex-java-cookie</i></td><td>ActiveX, Java, and cookie filtering.</td></tr><tr><td><i>dlp</i></td><td>DLP scanning.</td></tr><tr><td><i>fortiguard</i></td><td>FortiGuard web filtering.</td></tr><tr><td><i>range-block</i></td><td>Range block feature.</td></tr></table>	Option	Description	<i>av</i>	AntiVirus scanning.	<i>web-content</i>	Web filter content matching.	<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.	<i>dlp</i>	DLP scanning.	<i>fortiguard</i>	FortiGuard web filtering.	<i>range-block</i>	Range block feature.			
	Option	Description																
	<i>av</i>	AntiVirus scanning.																
	<i>web-content</i>	Web filter content matching.																
	<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.																
	<i>dlp</i>	DLP scanning.																
<i>fortiguard</i>	FortiGuard web filtering.																	
<i>range-block</i>	Range block feature.																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Pass single connection from all.		
	<i>antiphish</i>	AntiPhish credential checking.		
	<i>all</i>	Exempt from all security profiles.		
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	
referrer-host	Referrer host name.	string	Maximum length: 255	
status	Enable/disable this URL filter.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this URL filter.		
	<i>disable</i>	Disable this URL filter.		
type	Filter type (simple, regex, or wildcard).	option	-	simple
	Option	Description		
	<i>simple</i>	Simple URL string.		
	<i>regex</i>	Regular expression URL string.		
	<i>wildcard</i>	Wildcard URL string.		
url	URL to be filtered.	string	Maximum length: 511	
web-proxy-profile	Web proxy profile.	string	Maximum length: 63	

wireless-controller

This section includes syntax for the following commands:

- [config wireless-controller access-control-list on page 2413](#)
- [config wireless-controller ap-status on page 2417](#)
- [config wireless-controller apcfg-profile on page 2415](#)
- [config wireless-controller arrp-profile on page 2418](#)
- [config wireless-controller ble-profile on page 2421](#)
- [config wireless-controller bonjour-profile on page 2424](#)
- [config wireless-controller global on page 2426](#)
- [config wireless-controller hotspot20 anqp-3gpp-cellular on page 2431](#)
- [config wireless-controller hotspot20 anqp-ip-address-type on page 2432](#)
- [config wireless-controller hotspot20 anqp-nai-realm on page 2433](#)
- [config wireless-controller hotspot20 anqp-network-auth-type on page 2437](#)
- [config wireless-controller hotspot20 anqp-roaming-consortium on page 2438](#)
- [config wireless-controller hotspot20 anqp-venue-name on page 2439](#)
- [config wireless-controller hotspot20 anqp-venue-url on page 2439](#)
- [config wireless-controller hotspot20 h2qp-advice-of-charge on page 2440](#)
- [config wireless-controller hotspot20 h2qp-conn-capability on page 2442](#)
- [config wireless-controller hotspot20 h2qp-operator-name on page 2445](#)
- [config wireless-controller hotspot20 h2qp-osu-provider-nai on page 2447](#)
- [config wireless-controller hotspot20 h2qp-osu-provider on page 2445](#)
- [config wireless-controller hotspot20 h2qp-terms-and-conditions on page 2448](#)
- [config wireless-controller hotspot20 h2qp-wan-metric on page 2449](#)
- [config wireless-controller hotspot20 hs-profile on page 2450](#)
- [config wireless-controller hotspot20 icon on page 2458](#)
- [config wireless-controller hotspot20 qos-map on page 2459](#)
- [config wireless-controller inter-controller on page 2461](#)
- [config wireless-controller log on page 2463](#)
- [config wireless-controller mpsk-profile on page 2468](#)
- [config wireless-controller nac-profile on page 2471](#)
- [config wireless-controller qos-profile on page 2472](#)
- [config wireless-controller region on page 2475](#)
- [config wireless-controller setting on page 2476](#)
- [config wireless-controller snmp on page 2486](#)
- [config wireless-controller ssid-policy on page 2490](#)
- [config wireless-controller syslog-profile on page 2491](#)
- [config wireless-controller timers on page 2493](#)
- [config wireless-controller vap-group on page 2528](#)

- [config wireless-controller vap on page 2496](#)
- [config wireless-controller wag-profile on page 2529](#)
- [config wireless-controller wids-profile on page 2530](#)
- [config wireless-controller wtp-group on page 2571](#)
- [config wireless-controller wtp-profile on page 2574](#)
- [config wireless-controller wtp on page 2548](#)

config wireless-controller access-control-list

Configure WiFi bridge access control list.

```
config wireless-controller access-control-list
  Description: Configure WiFi bridge access control list.
  edit <name>
    set comment {string}
    config layer3-ipv4-rules
      Description: AP ACL layer3 ipv4 rule list.
      edit <rule-id>
        set action [allow|deny]
        set comment {string}
        set dstaddr {user}
        set dstport {integer}
        set protocol {integer}
        set srcaddr {user}
        set srcport {integer}
      next
    end
    config layer3-ipv6-rules
      Description: AP ACL layer3 ipv6 rule list.
      edit <rule-id>
        set action [allow|deny]
        set comment {string}
        set dstaddr {user}
        set dstport {integer}
        set protocol {integer}
        set srcaddr {user}
        set srcport {integer}
      next
    end
  next
end
```

config wireless-controller access-control-list

Parameter	Description	Type	Size	Default
comment	Description.	string	Maximum length: 63	
name	AP access control list name.	string	Maximum length: 35	

config layer3-ipv4-rules

Parameter	Description	Type	Size	Default						
action	Policy action (allow deny).	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allows traffic matching the policy.</td></tr><tr><td>deny</td><td>Blocks traffic matching the policy.</td></tr></table>	Option	Description	allow	Allows traffic matching the policy.	deny	Blocks traffic matching the policy.			
	Option	Description								
	allow	Allows traffic matching the policy.								
deny	Blocks traffic matching the policy.									
comment	Description.	string	Maximum length: 63							
dstaddr	Destination IP address (any local-LAN IPv4 address[/<network mask mask length>], default = any).	user	Not Specified							
dstport	Destination port (0 - 65535, default = 0, meaning any).	integer	Minimum value: 0 Maximum value: 65535	0						
protocol	Protocol type as defined by IANA (0 - 255, default = 255, meaning any).	integer	Minimum value: 0 Maximum value: 255	255						
rule-id	Rule ID (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	0						
srcaddr	Source IP address (any local-LAN IPv4 address [/<network mask mask length>], default = any).	user	Not Specified							
srcport	Source port (0 - 65535, default = 0, meaning any).	integer	Minimum value: 0 Maximum value: 65535	0						

config layer3-ipv6-rules

Parameter	Description	Type	Size	Default
action	Policy action (allow deny).	option	-	
	Option Description			
	<i>allow</i>	Allows traffic matching the policy.		
	<i>deny</i>	Blocks traffic matching the policy.		
comment	Description.	string	Maximum length: 63	
dstaddr	Destination IPv6 address (any local-LAN IPv6 address[/prefix length]), default = any.	user	Not Specified	
dstport	Destination port (0 - 65535, default = 0, meaning any).	integer	Minimum value: 0 Maximum value: 65535	0
protocol	Protocol type as defined by IANA (0 - 255, default = 255, meaning any).	integer	Minimum value: 0 Maximum value: 255	255
rule-id	Rule ID (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	0
srcaddr	Source IPv6 address (any local-LAN IPv6 address[/prefix length]), default = any.	user	Not Specified	
srcport	Source port (0 - 65535, default = 0, meaning any).	integer	Minimum value: 0 Maximum value: 65535	0

config wireless-controller apcfg-profile

Configure AP local configuration profiles.

```
config wireless-controller apcfg-profile
  Description: Configure AP local configuration profiles.
  edit <name>
    set ac-ip {ipv4-address}
```

```

set ac-port {integer}
set ac-timer {integer}
set ac-type [default|specify|...]
set ap-family [fap|fap-u|...]
config command-list
    Description: AP local configuration command list.
    edit <id>
        set name {string}
        set passwd-value {password}
        set type [non-password|password]
        set value {string}
    next
end
set comment {var-string}
next
end

```

config wireless-controller apcfg-profile

Parameter	Description	Type	Size	Default								
ac-ip	IP address of the validation controller that AP must be able to join after applying AP local configuration.	ipv4-address	Not Specified	0.0.0.0								
ac-port	Port of the validation controller that AP must be able to join after applying AP local configuration (1024 - 49150, default = 5246).	integer	Minimum value: 1024 Maximum value: 49150	5246								
ac-timer	Maximum waiting time for the AP to join the validation controller after applying AP local configuration (3 - 30 min, default = 10).	integer	Minimum value: 3 Maximum value: 30	10								
ac-type	Validation controller type (default = default).	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>This controller is the one and only controller that the AP could join after applying AP local configuration.</td></tr><tr><td>specify</td><td>Specified controller is the one and only controller that the AP could join after applying AP local configuration.</td></tr><tr><td>apcfg</td><td>Any controller defined by AP local configuration after applying AP local configuration.</td></tr></table>				Option	Description	default	This controller is the one and only controller that the AP could join after applying AP local configuration.	specify	Specified controller is the one and only controller that the AP could join after applying AP local configuration.	apcfg	Any controller defined by AP local configuration after applying AP local configuration.
Option	Description											
default	This controller is the one and only controller that the AP could join after applying AP local configuration.											
specify	Specified controller is the one and only controller that the AP could join after applying AP local configuration.											
apcfg	Any controller defined by AP local configuration after applying AP local configuration.											
ap-family	FortiAP family type (default = fap).	option	-	fap								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fap</i></td><td>FortiAP Family.</td></tr><tr><td><i>fap-u</i></td><td>FortiAP-U Family.</td></tr><tr><td><i>fap-c</i></td><td>FortiAP-C Family.</td></tr></table>				Option	Description	<i>fap</i>	FortiAP Family.	<i>fap-u</i>	FortiAP-U Family.	<i>fap-c</i>	FortiAP-C Family.
	Option	Description										
	<i>fap</i>	FortiAP Family.										
	<i>fap-u</i>	FortiAP-U Family.										
<i>fap-c</i>	FortiAP-C Family.											
comment	Comment.	var-string	Maximum length: 255									
name	AP local configuration profile name.	string	Maximum length: 35									

config command-list

Parameter	Description	Type	Size	Default						
id	Command ID.	integer	Minimum value: 1 Maximum value: 255	0						
name	AP local configuration command name.	string	Maximum length: 63							
passwd-value	AP local configuration command password value.	password	Not Specified							
type	The command type (default = non-password).	option	-	non-password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>non-password</i></td><td>Non-password command.</td></tr><tr><td><i>password</i></td><td>Password command.</td></tr></table>				Option	Description	<i>non-password</i>	Non-password command.	<i>password</i>	Password command.
Option	Description									
<i>non-password</i>	Non-password command.									
<i>password</i>	Password command.									
value	AP local configuration command value.	string	Maximum length: 127							

config wireless-controller ap-status

Configure access point status (rogue | accepted | suppressed).

```
config wireless-controller ap-status
  Description: Configure access point status (rogue | accepted | suppressed).
  edit <id>
    set bssid {mac-address}
    set ssid {string}
```

```

        set status [rogue|accepted|...]
    next
end

```

config wireless-controller ap-status

Parameter	Description	Type	Size	Default
bssid	Access Point's (AP's) BSSID.	mac-address	Not Specified	00:00:00:00:00:00
id	AP ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ssid	Access Point's (AP's) SSID.	string	Maximum length: 32	
status	Access Point's (AP's) status: rogue, accepted, or suppressed.	option	-	rogue
	Option	Description		
	rogue	Rogue AP.		
	accepted	Accepted AP.		
	suppressed	Suppressed AP.		

config wireless-controller arrp-profile

Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.

```

config wireless-controller arrp-profile
    Description: Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.
    edit <name>
        set comment {var-string}
        set darrp-optimize {integer}
        set darrp-optimize-schedules <name1>, <name2>, ...
        set include-dfs-channel [enable|disable]
        set include-weather-channel [enable|disable]
        set monitor-period {integer}
        set override-darrp-optimize [enable|disable]
        set selection-period {integer}
        set threshold-ap {integer}
        set threshold-channel-load {integer}
        set threshold-noise-floor {string}
        set threshold-rx-errors {integer}
        set threshold-spectral-rssi {string}
    end
end

```

```

set threshold-tx-retries {integer}
set weight-channel-load {integer}
set weight-dfs-channel {integer}
set weight-managed-ap {integer}
set weight-noise-floor {integer}
set weight-rogue-ap {integer}
set weight-spectral-rssi {integer}
set weight-weather-channel {integer}
next
end

```

config wireless-controller arrp-profile

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
darrp-optimize	Time for running Distributed Automatic Radio Resource Provisioning (DARRP) optimizations (0 - 86400 sec, default = 86400, 0 = disable).	integer	Minimum value: 0 Maximum value: 86400	86400						
darrp-optimize-schedules <name>	Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35							
include-dfs-channel	Enable/disable use of DFS channel in DARRP channel selection phase 1 (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Include DFS channel in darrp channel selection phase 1.</td></tr><tr><td>disable</td><td>Exclude DFS channel in darrp channel selection phase 1.</td></tr></table>				Option	Description	enable	Include DFS channel in darrp channel selection phase 1.	disable	Exclude DFS channel in darrp channel selection phase 1.
Option	Description									
enable	Include DFS channel in darrp channel selection phase 1.									
disable	Exclude DFS channel in darrp channel selection phase 1.									
include-weather-channel	Enable/disable use of weather channel in DARRP channel selection phase 1 (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Include weather channel in darrp channel selection phase 1.</td></tr><tr><td>disable</td><td>Exclude weather channel in darrp channel selection phase 1.</td></tr></table>				Option	Description	enable	Include weather channel in darrp channel selection phase 1.	disable	Exclude weather channel in darrp channel selection phase 1.
Option	Description									
enable	Include weather channel in darrp channel selection phase 1.									
disable	Exclude weather channel in darrp channel selection phase 1.									

Parameter	Description	Type	Size	Default						
monitor-period	Period in seconds to measure average transmit retries and receive errors (default = 300).	integer	Minimum value: 0 Maximum value: 65535	300						
name	WiFi ARRP profile name.	string	Maximum length: 35							
override-darrp-optimize	Enable to override setting darrp-optimize and darrp-optimize-schedules (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override setting darrp-optimize and darrp-optimize-schedules.</td></tr><tr><td>disable</td><td>Use setting darrp-optimize and darrp-optimize-schedules.</td></tr></table>				Option	Description	enable	Override setting darrp-optimize and darrp-optimize-schedules.	disable	Use setting darrp-optimize and darrp-optimize-schedules.
Option	Description									
enable	Override setting darrp-optimize and darrp-optimize-schedules.									
disable	Use setting darrp-optimize and darrp-optimize-schedules.									
selection-period	Period in seconds to measure average channel load, noise floor, spectral RSSI (default = 3600).	integer	Minimum value: 0 Maximum value: 65535	3600						
threshold-ap	Threshold to reject channel in DARRP channel selection phase 1 due to surrounding APs (0 - 500, default = 250).	integer	Minimum value: 0 Maximum value: 500	250						
threshold-channel-load	Threshold in percentage to reject channel in DARRP channel selection phase 1 due to channel load (0 - 100, default = 60).	integer	Minimum value: 0 Maximum value: 100	60						
threshold-noise-floor	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to noise floor (-95 to -20, default = -85).	string	Maximum length: 7	-85						
threshold-rx-errors	Threshold in percentage for receive errors to trigger channel reselection in DARRP monitor stage (0 - 100, default = 50).	integer	Minimum value: 0 Maximum value: 100	50						
threshold-spectral-rssi	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to spectral RSSI (-95 to -20, default = -65).	string	Maximum length: 7	-65						

Parameter	Description	Type	Size	Default
threshold-tx-retries	Threshold in percentage for transmit retries to trigger channel reselection in DARRP monitor stage (0 - 1000, default = 300).	integer	Minimum value: 0 Maximum value: 1000	300
weight-channel-load	Weight in DARRP channel score calculation for channel load (0 - 2000, default = 20).	integer	Minimum value: 0 Maximum value: 2000	20
weight-dfs-channel	Weight in DARRP channel score calculation for DFS channel (0 - 2000, default = 0).	integer	Minimum value: 0 Maximum value: 2000	0
weight-managed-ap	Weight in DARRP channel score calculation for managed APs (0 - 2000, default = 50).	integer	Minimum value: 0 Maximum value: 2000	50
weight-noise-floor	Weight in DARRP channel score calculation for noise floor (0 - 2000, default = 40).	integer	Minimum value: 0 Maximum value: 2000	40
weight-rogue-ap	Weight in DARRP channel score calculation for rogue APs (0 - 2000, default = 10).	integer	Minimum value: 0 Maximum value: 2000	10
weight-spectral-rssi	Weight in DARRP channel score calculation for spectral RSSI (0 - 2000, default = 40).	integer	Minimum value: 0 Maximum value: 2000	40
weight-weather-channel	Weight in DARRP channel score calculation for weather channel (0 - 2000, default = 0).	integer	Minimum value: 0 Maximum value: 2000	0

config wireless-controller ble-profile

Configure Bluetooth Low Energy profile.

```

config wireless-controller ble-profile
  Description: Configure Bluetooth Low Energy profile.
  edit <name>
    set advertising {option1}, {option2}, ...
    set beacon-interval {integer}

```

```

set ble-scanning [enable|disable]
set comment {string}
set eddystone-instance {string}
set eddystone-namespace {string}
set eddystone-url {string}
set ibeacon-uuid {string}
set major-id {integer}
set minor-id {integer}
set scan-interval {integer}
set scan-period {integer}
set scan-threshold {string}
set scan-time {integer}
set scan-type [active|passive]
set scan-window {integer}
set txpower [0|1|...]
next
end

```

config wireless-controller ble-profile

Parameter	Description	Type	Size	Default								
advertising	Advertising type.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ibeacon</i></td><td>iBeacon advertising.</td></tr><tr><td><i>eddystone-uid</i></td><td>Eddystone UID advertising.</td></tr><tr><td><i>eddystone-url</i></td><td>Eddystone URL advertising.</td></tr></table>	Option	Description	<i>ibeacon</i>	iBeacon advertising.	<i>eddystone-uid</i>	Eddystone UID advertising.	<i>eddystone-url</i>	Eddystone URL advertising.			
Option	Description											
<i>ibeacon</i>	iBeacon advertising.											
<i>eddystone-uid</i>	Eddystone UID advertising.											
<i>eddystone-url</i>	Eddystone URL advertising.											
beacon-interval	Beacon interval (default = 100 msec).	integer	Minimum value: 40 Maximum value: 3500	100								
ble-scanning	Enable/disable Bluetooth Low Energy (BLE) scanning.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable BLE scanning.</td></tr><tr><td><i>disable</i></td><td>Disable BLE scanning.</td></tr></table>	Option	Description	<i>enable</i>	Enable BLE scanning.	<i>disable</i>	Disable BLE scanning.					
Option	Description											
<i>enable</i>	Enable BLE scanning.											
<i>disable</i>	Disable BLE scanning.											
comment	Comment.	string	Maximum length: 63									
eddystone-instance	Eddystone instance ID.	string	Maximum length: 12	abcdef								

Parameter	Description	Type	Size	Default
eddystone-namespace	Eddystone namespace ID.	string	Maximum length: 20	0102030405
eddystone-url	Eddystone URL.	string	Maximum length: 127	http://www.fortinet.com
ibeacon-uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 63	005ea414-cbd1-11e5-9956-625662870761
major-id	Major ID.	integer	Minimum value: 0 Maximum value: 65535	1000
minor-id	Minor ID.	integer	Minimum value: 0 Maximum value: 65535	2000
name	Bluetooth Low Energy profile name.	string	Maximum length: 35	
scan-interval	Scan Interval (default = 50 msec).	integer	Minimum value: 10 Maximum value: 1000	50
scan-period	Scan Period (default = 4000 msec).	integer	Minimum value: 1000 Maximum value: 10000	4000
scan-threshold	Minimum signal level/threshold in dBm required for the AP to report detected BLE device (-95 to -20, default = -90).	string	Maximum length: 7	-90
scan-time	Scan Time (default = 1000 msec).	integer	Minimum value: 1000 Maximum value: 10000	1000
scan-type	Scan Type (default = active).	option	-	active

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>active</td><td>Active BLE scanning.</td></tr><tr><td>passive</td><td>Passive BLE scanning.</td></tr></table>	Option	Description	active	Active BLE scanning.	passive	Passive BLE scanning.																									
	Option	Description																														
	active	Active BLE scanning.																														
passive	Passive BLE scanning.																															
scan-window	Scan Windows (default = 50 msec).	integer	Minimum value: 10 Maximum value: 1000	50																												
txpower	Transmit power level (default = 0).	option	-	0																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>Transmit power level 0 (-21 dBm)</td></tr><tr><td>1</td><td>Transmit power level 1 (-18 dBm)</td></tr><tr><td>2</td><td>Transmit power level 2 (-15 dBm)</td></tr><tr><td>3</td><td>Transmit power level 3 (-12 dBm)</td></tr><tr><td>4</td><td>Transmit power level 4 (-9 dBm)</td></tr><tr><td>5</td><td>Transmit power level 5 (-6 dBm)</td></tr><tr><td>6</td><td>Transmit power level 6 (-3 dBm)</td></tr><tr><td>7</td><td>Transmit power level 7 (0 dBm)</td></tr><tr><td>8</td><td>Transmit power level 8 (1 dBm)</td></tr><tr><td>9</td><td>Transmit power level 9 (2 dBm)</td></tr><tr><td>10</td><td>Transmit power level 10 (3 dBm)</td></tr><tr><td>11</td><td>Transmit power level 11 (4 dBm)</td></tr><tr><td>12</td><td>Transmit power level 12 (5 dBm)</td></tr></table>	Option	Description	0	Transmit power level 0 (-21 dBm)	1	Transmit power level 1 (-18 dBm)	2	Transmit power level 2 (-15 dBm)	3	Transmit power level 3 (-12 dBm)	4	Transmit power level 4 (-9 dBm)	5	Transmit power level 5 (-6 dBm)	6	Transmit power level 6 (-3 dBm)	7	Transmit power level 7 (0 dBm)	8	Transmit power level 8 (1 dBm)	9	Transmit power level 9 (2 dBm)	10	Transmit power level 10 (3 dBm)	11	Transmit power level 11 (4 dBm)	12	Transmit power level 12 (5 dBm)			
	Option	Description																														
	0	Transmit power level 0 (-21 dBm)																														
	1	Transmit power level 1 (-18 dBm)																														
	2	Transmit power level 2 (-15 dBm)																														
	3	Transmit power level 3 (-12 dBm)																														
	4	Transmit power level 4 (-9 dBm)																														
	5	Transmit power level 5 (-6 dBm)																														
	6	Transmit power level 6 (-3 dBm)																														
	7	Transmit power level 7 (0 dBm)																														
	8	Transmit power level 8 (1 dBm)																														
	9	Transmit power level 9 (2 dBm)																														
	10	Transmit power level 10 (3 dBm)																														
11	Transmit power level 11 (4 dBm)																															
12	Transmit power level 12 (5 dBm)																															

config wireless-controller bonjour-profile

Configure Bonjour profiles. Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour.

```
config wireless-controller bonjour-profile
  Description: Configure Bonjour profiles. Bonjour is Apple's zero configuration networking
  protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour.
  edit <name>
    set comment {string}
    set micro-location [enable|disable]
    config policy-list
```



```

        Description: Bonjour policy list.
    edit <policy-id>
        set description {string}
        set from-vlan {string}
        set services {option1}, {option2}, ...
        set to-vlan {string}
    next
end
next
end

```

config wireless-controller bonjour-profile

Parameter	Description	Type	Size	Default						
comment	Comment.	string	Maximum length: 63							
micro-location	Enable/disable Micro location for Bonjour profile (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Micro location.</td></tr><tr><td><i>disable</i></td><td>Disable Micro location.</td></tr></table>				Option	Description	<i>enable</i>	Enable Micro location.	<i>disable</i>	Disable Micro location.
	Option	Description								
	<i>enable</i>	Enable Micro location.								
<i>disable</i>	Disable Micro location.									
name	Bonjour profile name.	string	Maximum length: 35							

config policy-list

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
from-vlan	VLAN ID from which the Bonjour service is advertised (0 - 4094, default = 0).	string	Maximum length: 63	0
policy-id	Policy ID.	integer	Minimum value: 1 Maximum value: 65535	0
services	Bonjour services for the VLAN connecting to the Bonjour network.	option	-	all

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>All services.</td></tr><tr><td><i>airplay</i></td><td>AirPlay.</td></tr><tr><td><i>afp</i></td><td>AFP (Apple File Sharing).</td></tr><tr><td><i>bit-torrent</i></td><td>BitTorrent.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>ichat</i></td><td>iChat.</td></tr><tr><td><i>itunes</i></td><td>iTunes.</td></tr><tr><td><i>printers</i></td><td>Printers.</td></tr><tr><td><i>samba</i></td><td>Samba.</td></tr><tr><td><i>scanners</i></td><td>Scanners.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr><tr><td><i>chromecast</i></td><td>ChromeCast.</td></tr><tr><td><i>miracast</i></td><td>Miracast.</td></tr></table>	Option	Description	<i>all</i>	All services.	<i>airplay</i>	AirPlay.	<i>afp</i>	AFP (Apple File Sharing).	<i>bit-torrent</i>	BitTorrent.	<i>ftp</i>	FTP.	<i>ichat</i>	iChat.	<i>itunes</i>	iTunes.	<i>printers</i>	Printers.	<i>samba</i>	Samba.	<i>scanners</i>	Scanners.	<i>ssh</i>	SSH.	<i>chromecast</i>	ChromeCast.	<i>miracast</i>	Miracast.			
	Option	Description																														
	<i>all</i>	All services.																														
	<i>airplay</i>	AirPlay.																														
	<i>afp</i>	AFP (Apple File Sharing).																														
	<i>bit-torrent</i>	BitTorrent.																														
	<i>ftp</i>	FTP.																														
	<i>ichat</i>	iChat.																														
	<i>itunes</i>	iTunes.																														
	<i>printers</i>	Printers.																														
	<i>samba</i>	Samba.																														
	<i>scanners</i>	Scanners.																														
	<i>ssh</i>	SSH.																														
	<i>chromecast</i>	ChromeCast.																														
<i>miracast</i>	Miracast.																															
to-vlan	VLAN ID to which the Bonjour service is made available (0 - 4094, default = all).	string	Maximum length: 63	all																												

config wireless-controller global

Configure wireless controller global settings.

```

config wireless-controller global
  Description: Configure wireless controller global settings.
  set acd-process-count {integer}
  set ap-log-server [enable|disable]
  set ap-log-server-ip {ipv4-address}
  set ap-log-server-port {integer}
  set control-message-offload {option1}, {option2}, ...
  set data-ethernet-II [enable|disable]
  set dfs-lab-test [enable|disable]
  set discovery-mc-addr {ipv4-address-multicast}
  set fiapp-eth-type {integer}
  set image-download [enable|disable]
  set ipsec-base-ip {ipv4-address}
  set link-aggregation [enable|disable]
  set local-radio-vdom {string}
  set location {string}
  set max-ble-device {integer}
  set max-clients {integer}

```

```

set max-retransmit {integer}
set max-rogue-ap {integer}
set max-rogue-ap-wtp {integer}
set max-rogue-sta {integer}
set max-sta-cap {integer}
set max-sta-cap-wtp {integer}
set max-sta-offline {integer}
set max-sta-offline-ip2mac {integer}
set max-wids-entry {integer}
set mesh-eth-type {integer}
set nac-interval {integer}
set name {string}
set rogue-scan-mac-adjacency {integer}
set rolling-wtp-upgrade [enable|disable]
set rolling-wtp-upgrade-threshold {string}
set tunnel-mode [compatible|strict]
set wpad-process-count {integer}
set wtp-share [enable|disable]
end

```

config wireless-controller global

Parameter	Description	Type	Size	Default
acd-process-count	Configure the number cw_acd daemons for multi-core CPU support (default = 0).	integer	Minimum value: 0 Maximum value: 255	0
ap-log-server	Enable/disable configuring FortiGate to redirect wireless event log messages or FortiAPs to send UTM log messages to a syslog server (default = disable).	option	-	disable
	Option	Description		
	enable	Enable AP log server.		
	disable	Disable AP log server.		
ap-log-server-ip	IP address that FortiGate or FortiAPs send log messages to.	ipv4-address	Not Specified	0.0.0.0
ap-log-server-port	Port that FortiGate or FortiAPs send log messages to.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default																				
control-message-offload	Configure CAPWAP control message data channel offload.	option	-	ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health spectral-analysis																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ebp-frame</td><td>Ekahau blink protocol (EBP) frames.</td></tr><tr><td>aeroscout-tag</td><td>AeroScout tag.</td></tr><tr><td>ap-list</td><td>Rogue AP list.</td></tr><tr><td>sta-list</td><td>Rogue STA list.</td></tr><tr><td>sta-cap-list</td><td>STA capability list.</td></tr><tr><td>stats</td><td>WTP, radio, VAP, and STA statistics.</td></tr><tr><td>aeroscout-mu</td><td>AeroScout Mobile Unit (MU) report.</td></tr><tr><td>sta-health</td><td>STA health log.</td></tr><tr><td>spectral-analysis</td><td>Spectral analysis report.</td></tr></table>				Option	Description	ebp-frame	Ekahau blink protocol (EBP) frames.	aeroscout-tag	AeroScout tag.	ap-list	Rogue AP list.	sta-list	Rogue STA list.	sta-cap-list	STA capability list.	stats	WTP, radio, VAP, and STA statistics.	aeroscout-mu	AeroScout Mobile Unit (MU) report.	sta-health	STA health log.	spectral-analysis	Spectral analysis report.
Option	Description																							
ebp-frame	Ekahau blink protocol (EBP) frames.																							
aeroscout-tag	AeroScout tag.																							
ap-list	Rogue AP list.																							
sta-list	Rogue STA list.																							
sta-cap-list	STA capability list.																							
stats	WTP, radio, VAP, and STA statistics.																							
aeroscout-mu	AeroScout Mobile Unit (MU) report.																							
sta-health	STA health log.																							
spectral-analysis	Spectral analysis report.																							
data-ethernet-II	Configure the wireless controller to use Ethernet II or 802.3 frames with 802.3 data tunnel mode (default = enable).	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Use Ethernet II frames with 802.3 data tunnel mode.</td></tr><tr><td>disable</td><td>Use 802.3 Ethernet frames with 802.3 data tunnel mode.</td></tr></table>				Option	Description	enable	Use Ethernet II frames with 802.3 data tunnel mode.	disable	Use 802.3 Ethernet frames with 802.3 data tunnel mode.														
Option	Description																							
enable	Use Ethernet II frames with 802.3 data tunnel mode.																							
disable	Use 802.3 Ethernet frames with 802.3 data tunnel mode.																							
dfs-lab-test	Enable/disable DFS certificate lab test mode.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DFS certificate lab test mode.</td></tr><tr><td>disable</td><td>Disable DFS certificate lab test mode.</td></tr></table>				Option	Description	enable	Enable DFS certificate lab test mode.	disable	Disable DFS certificate lab test mode.														
Option	Description																							
enable	Enable DFS certificate lab test mode.																							
disable	Disable DFS certificate lab test mode.																							
discovery-mc-addr	Multicast IP address for AP discovery (default = 244.0.1.140).	ipv4-address-multicast	Not Specified	224.0.1.140																				

Parameter	Description	Type	Size	Default						
fiapp-eth-type	Ethernet type for Fortinet Inter-Access Point Protocol (IAPP), or IEEE 802.11f, packets (0 - 65535, default = 5252).	integer	Minimum value: 0 Maximum value: 65535	5252						
image-download	Enable/disable WTP image download at join time.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WTP image download at join time.</td></tr><tr><td>disable</td><td>Disable WTP image download at join time.</td></tr></table>				Option	Description	enable	Enable WTP image download at join time.	disable	Disable WTP image download at join time.
	Option	Description								
	enable	Enable WTP image download at join time.								
disable	Disable WTP image download at join time.									
ipsec-base-ip	Base IP address for IPsec VPN tunnels between the access points and the wireless controller (default = 169.254.0.1).	ipv4-address	Not Specified	169.254.0.1						
link-aggregation	Enable/disable calculating the CAPWAP transmit hash to load balance sessions to link aggregation nodes (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable calculating the CAPWAP transmit hash.</td></tr><tr><td>disable</td><td>Disable calculating the CAPWAP transmit hash.</td></tr></table>				Option	Description	enable	Enable calculating the CAPWAP transmit hash.	disable	Disable calculating the CAPWAP transmit hash.
	Option	Description								
	enable	Enable calculating the CAPWAP transmit hash.								
disable	Disable calculating the CAPWAP transmit hash.									
local-radio-vdom *	Assign local radio's virtual domain.	string	Maximum length: 31	root						
location	Description of the location of the wireless controller.	string	Maximum length: 35							
max-ble-device	Maximum number of BLE devices stored on the controller (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-clients	Maximum number of clients that can connect simultaneously (default = 0, meaning no limitation).	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-retransmit	Maximum number of tunnel packet retransmissions (0 - 64, default = 3).	integer	Minimum value: 0 Maximum value: 64	3						
max-rogue-ap	Maximum number of rogue APs stored on the controller (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0						

Parameter	Description	Type	Size	Default
max-rogue-ap-wtp	Maximum number of rogue AP's wtp info stored on the controller (1 - 16, default = 16).	integer	Minimum value: 1 Maximum value: 16	16
max-rogue-sta	Maximum number of rogue stations stored on the controller (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
max-sta-cap	Maximum number of station cap stored on the controller (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
max-sta-cap-wtp	Maximum number of station cap's wtp info stored on the controller (1 - 16, default = 8).	integer	Minimum value: 1 Maximum value: 8	8
max-sta-offline	Maximum number of station offline stored on the controller (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
max-sta-offline-ip2mac	Maximum number of station offline ip2mac stored on the controller (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
max-wids-entry	Maximum number of wids entries stored on the controller (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
mesh-eth-type	Mesh Ethernet identifier included in backhaul packets (0 - 65535, default = 8755).	integer	Minimum value: 0 Maximum value: 65535	8755
nac-interval	Interval in seconds between two WiFi network access control (NAC) checks (10 - 600, default = 120).	integer	Minimum value: 10 Maximum value: 600	120
name	Name of the wireless controller.	string	Maximum length: 35	
rogue-scan-mac-adjacency	Maximum numerical difference between an AP's Ethernet and wireless MAC values to match for rogue detection (0 - 31, default = 7).	integer	Minimum value: 0 Maximum value: 31	7
rolling-wtp-upgrade	Enable/disable rolling WTP upgrade (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable rolling WTP upgrade.		
	<i>disable</i>	Disable rolling WTP upgrade.		
rolling-wtp-upgrade-threshold	Minimum signal level/threshold in dBm required for the managed WTP to be included in rolling WTP upgrade (-95 to -20, default = -80).	string	Maximum length: 7	-80
tunnel-mode	Compatible/strict tunnel mode.	option	-	compatible
	Option	Description		
	<i>compatible</i>	Allow for backward compatible ciphers(3DES+SHA1+Strong list).		
	<i>strict</i>	Follow system level strong-crypto ciphers.		
wpad-process-count	Wpad daemon process count for multi-core CPU support.	integer	Minimum value: 0 0 Maximum value: 255	0
wtp-share	Enable/disable sharing of WTPs between VDOMs.	option	-	disable
	Option	Description		
	<i>enable</i>	WTP can be shared between all VDOMs.		
	<i>disable</i>	WTP can be used only in its own VDOM.		

* This parameter may not exist in some models.

config wireless-controller hotspot20 anqp-3gpp-cellular

Configure 3GPP public land mobile network (PLMN).

```

config wireless-controller hotspot20 anqp-3gpp-cellular
  Description: Configure 3GPP public land mobile network (PLMN).
  edit <name>
    config mcc-mnc-list
      Description: Mobile Country Code and Mobile Network Code configuration.
      edit <id>
        set mcc {string}
        set mnc {string}
      next
    end
  next
end

```

config wireless-controller hotspot20 anqp-3gpp-cellular

Parameter	Description	Type	Size	Default
name	3GPP PLMN name.	string	Maximum length: 35	

config mcc-mnc-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 1 Maximum value: 6	0
mcc	Mobile country code.	string	Maximum length: 3	
mnc	Mobile network code.	string	Maximum length: 3	

config wireless-controller hotspot20 anqp-ip-address-type

Configure IP address type availability.

```
config wireless-controller hotspot20 anqp-ip-address-type
  Description: Configure IP address type availability.
  edit <name>
    set ipv4-address-type [not-available|public|...]
    set ipv6-address-type [not-available|available|...]
  next
end
```

config wireless-controller hotspot20 anqp-ip-address-type

Parameter	Description	Type	Size	Default
ipv4-address-type	IPv4 address type.	option	-	not-available
Option	Description			
not-available	Address type not available.			

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>public</i></td><td>Public IPv4 address available.</td></tr><tr><td><i>port-restricted</i></td><td>Port-restricted IPv4 address available.</td></tr><tr><td><i>single-NATed-private</i></td><td>Single NATed private IPv4 address available.</td></tr><tr><td><i>double-NATed-private</i></td><td>Double NATed private IPv4 address available.</td></tr><tr><td><i>port-restricted-and-single-NATed</i></td><td>Port-restricted IPv4 address and single NATed IPv4 address available.</td></tr><tr><td><i>port-restricted-and-double-NATed</i></td><td>Port-restricted IPv4 address and double NATed IPv4 address available.</td></tr><tr><td><i>not-known</i></td><td>Availability of the address type is not known.</td></tr></table>	Option	Description	<i>public</i>	Public IPv4 address available.	<i>port-restricted</i>	Port-restricted IPv4 address available.	<i>single-NATed-private</i>	Single NATed private IPv4 address available.	<i>double-NATed-private</i>	Double NATed private IPv4 address available.	<i>port-restricted-and-single-NATed</i>	Port-restricted IPv4 address and single NATed IPv4 address available.	<i>port-restricted-and-double-NATed</i>	Port-restricted IPv4 address and double NATed IPv4 address available.	<i>not-known</i>	Availability of the address type is not known.			
	Option	Description																		
	<i>public</i>	Public IPv4 address available.																		
	<i>port-restricted</i>	Port-restricted IPv4 address available.																		
	<i>single-NATed-private</i>	Single NATed private IPv4 address available.																		
	<i>double-NATed-private</i>	Double NATed private IPv4 address available.																		
	<i>port-restricted-and-single-NATed</i>	Port-restricted IPv4 address and single NATed IPv4 address available.																		
<i>port-restricted-and-double-NATed</i>	Port-restricted IPv4 address and double NATed IPv4 address available.																			
<i>not-known</i>	Availability of the address type is not known.																			
ipv6-address-type	IPv6 address type.	option	-	not-available																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>not-available</i></td><td>Address type not available.</td></tr><tr><td><i>available</i></td><td>Address type available.</td></tr><tr><td><i>not-known</i></td><td>Availability of the address type not known.</td></tr></table>	Option	Description	<i>not-available</i>	Address type not available.	<i>available</i>	Address type available.	<i>not-known</i>	Availability of the address type not known.											
	Option	Description																		
	<i>not-available</i>	Address type not available.																		
	<i>available</i>	Address type available.																		
<i>not-known</i>	Availability of the address type not known.																			
name	IP type name.	string	Maximum length: 35																	

config wireless-controller hotspot20 anqp-nai-realm

Configure network access identifier (NAI) realm.

```

config wireless-controller hotspot20 anqp-nai-realm
  Description: Configure network access identifier (NAI) realm.
  edit <name>
    config nai-list
      Description: NAI list.
      edit <name>
        config eap-method
          Description: EAP Methods.
          edit <index>
            config auth-param
              Description: EAP auth param.

```

```

        edit <index>
            set id [non-eap-inner-auth|inner-auth-eap|...]
            set val [eap-identity|eap-md5|...]
        next
    end
    set method [eap-identity|eap-md5|...]
next
end
set encoding [disable|enable]
set nai-realm {string}
next
end
next
end

```

config wireless-controller hotspot20 anqp-nai-realm

Parameter	Description	Type	Size	Default
name	NAI realm list name.	string	Maximum length: 35	

config nai-list

Parameter	Description	Type	Size	Default
encoding	Enable/disable format in accordance with IETF RFC 4282.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable format in accordance with IETF RFC 4282.		
	<i>enable</i>	Enable format in accordance with IETF RFC 4282.		
nai-realm	Configure NAI realms (delimited by a semi-colon character).	string	Maximum length: 255	
name	NAI realm name.	string	Maximum length: 35	

config eap-method

Parameter	Description	Type	Size	Default
index	EAP method index.	integer	Minimum value: 1 Maximum value: 5	0

Parameter	Description	Type	Size	Default
method	EAP method type.	option	-	eap-identity
	Option	Description		
	<i>eap-identity</i>	Identity.		
	<i>eap-md5</i>	MD5.		
	<i>eap-tls</i>	TLS.		
	<i>eap-ttls</i>	TTLS.		
	<i>eap-peap</i>	PEAP.		
	<i>eap-sim</i>	SIM.		
	<i>eap-aka</i>	AKA.		
	<i>eap-aka-prime</i>	AKA'.		

config auth-param

Parameter	Description	Type	Size	Default
id	ID of authentication parameter.	option	-	inner-auth-eap
	Option	Description		
	<i>non-eap-inner-auth</i>	Non-EAP inner authentication type.		
	<i>inner-auth-eap</i>	Inner authentication EAP method type.		
	<i>credential</i>	Credential type.		
	<i>tunneled-credential</i>	Tunneled EAP method credential type.		
index	Param index.	integer	Minimum value: 1 Maximum value: 4	0
val	Value of authentication parameter.	option	-	eap-identity
	Option	Description		
	<i>eap-identity</i>	EAP Identity.		
	<i>eap-md5</i>	EAP MD5.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>eap-tls</i>	EAP TLS.		
	<i>eap-ttls</i>	EAP TTLS.		
	<i>eap-peap</i>	EAP PEAP.		
	<i>eap-sim</i>	EAP SIM.		
	<i>eap-aka</i>	EAP AKA.		
	<i>eap-aka-prime</i>	EAP AKA'.		
	<i>non-eap-pap</i>	Non EAP PAP.		
	<i>non-eap-chap</i>	Non EAP CHAP.		
	<i>non-eap-mschap</i>	Non EAP MSCHAP.		
	<i>non-eap-mschapv2</i>	Non EAP MSCHAPV2.		
	<i>cred-sim</i>	Credential SIM.		
	<i>cred-usim</i>	Credential USIM.		
	<i>cred-nfc</i>	Credential NFC secure element.		
	<i>cred-hardware-token</i>	Credential hardware token.		
	<i>cred-softoken</i>	Credential softoken.		
	<i>cred-certificate</i>	Credential certificate.		
	<i>cred-user-pwd</i>	Credential username password.		
	<i>cred-none</i>	Credential none.		
	<i>cred-vendor-specific</i>	Credential vendor specific.		
	<i>tun-cred-sim</i>	Tunneled credential SIM.		
	<i>tun-cred-usim</i>	Tunneled credential USIM.		
	<i>tun-cred-nfc</i>	Tunneled credential NFC secure element.		
	<i>tun-cred-hardware-token</i>	Tunneled credential hardware token.		
	<i>tun-cred-softoken</i>	Tunneled credential softoken.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tun-cred-certificate</i>	Tunneled credential certificate.		
	<i>tun-cred-user-pwd</i>	Tunneled credential username password.		
	<i>tun-cred-anonymous</i>	Tunneled credential anonymous.		
	<i>tun-cred-vendor-specific</i>	Tunneled credential vendor specific.		

config wireless-controller hotspot20 anqp-network-auth-type

Configure network authentication type.

```
config wireless-controller hotspot20 anqp-network-auth-type
  Description: Configure network authentication type.
  edit <name>
    set auth-type [acceptance-of-terms|online-enrollment|...]
    set url {string}
  next
end
```

config wireless-controller hotspot20 anqp-network-auth-type

Parameter	Description	Type	Size	Default
auth-type	Network authentication type.	option	-	acceptance-of-terms
	Option	Description		
	<i>acceptance-of-terms</i>	Acceptance of terms and conditions.		
	<i>online-enrollment</i>	Online enrollment supported.		
	<i>http-redirection</i>	HTTP and HTTPS redirection.		
	<i>dns-redirection</i>	DNS redirection.		

Parameter	Description	Type	Size	Default
name	Authentication type name.	string	Maximum length: 35	
url	Redirect URL.	string	Maximum length: 255	

config wireless-controller hotspot20 anqp-roaming-consortium

Configure roaming consortium.

```

config wireless-controller hotspot20 anqp-roaming-consortium
  Description: Configure roaming consortium.
  edit <name>
    config oi-list
      Description: Organization identifier list.
      edit <index>
        set comment {string}
        set oi {string}
      next
    end
  next
end

```

config wireless-controller hotspot20 anqp-roaming-consortium

Parameter	Description	Type	Size	Default
name	Roaming consortium name.	string	Maximum length: 35	

config oi-list

Parameter	Description	Type	Size	Default
comment	Comment.	string	Maximum length: 35	
index	OI index.	integer	Minimum value: 1 Maximum value: 10	0
oi	Organization identifier.	string	Maximum length: 10	

config wireless-controller hotspot20 anqp-venue-name

Configure venue name duple.

```
config wireless-controller hotspot20 anqp-venue-name
  Description: Configure venue name duple.
  edit <name>
    config value-list
      Description: Name list.
      edit <index>
        set lang {string}
        set value {string}
      next
    end
  next
end
```

config wireless-controller hotspot20 anqp-venue-name

Parameter	Description	Type	Size	Default
name	Name of venue name duple.	string	Maximum length: 35	

config value-list

Parameter	Description	Type	Size	Default
index	Value index.	integer	Minimum value: 1 Maximum value: 10	0
lang	Language code.	string	Maximum length: 3	eng
value	Venue name value.	string	Maximum length: 252	

config wireless-controller hotspot20 anqp-venue-url

Configure venue URL.

```
config wireless-controller hotspot20 anqp-venue-url
  Description: Configure venue URL.
  edit <name>
    config value-list
```

```

        Description: URL list.
        edit <index>
            set number {integer}
            set value {string}
        next
    end
next
end

```

config wireless-controller hotspot20 anqp-venue-url

Parameter	Description	Type	Size	Default
name	Name of venue url.	string	Maximum length: 35	

config value-list

Parameter	Description	Type	Size	Default
index	URL index.	integer	Minimum value: 1 Maximum value: 10	0
number	Venue number.	integer	Minimum value: 0 Maximum value: 255	0
value	Venue URL value.	string	Maximum length: 254	

config wireless-controller hotspot20 h2qp-advice-of-charge

Configure advice of charge.

```

config wireless-controller hotspot20 h2qp-advice-of-charge
    Description: Configure advice of charge.
    edit <name>
        config aoc-list
            Description: AOC list.
            edit <name>
                set nai-realm {string}
                set nai-realm-encoding {string}
            config plan-info

```



```

        Description: Plan info.
        edit <name>
            set currency {string}
            set info-file {string}
            set lang {string}
        next
    end
    set type [time-based|volume-based|...]
next
end
next
end

```

config wireless-controller hotspot20 h2qp-advice-of-charge

Parameter	Description	Type	Size	Default
name	Plan name.	string	Maximum length: 35	

config aoc-list

Parameter	Description	Type	Size	Default
nai-realm	NAI realm list name.	string	Maximum length: 255	
nai-realm-encoding	NAI realm encoding.	string	Maximum length: 1	
name	Advice of charge ID.	string	Maximum length: 35	
type	Usage charge type.	option	-	time-based

Option	Description
<i>time-based</i>	Time based usage charge.
<i>volume-based</i>	Volume based usage charge.
<i>time-and-volume-based</i>	Time and volume based usage charge.
<i>unlimited</i>	Unlimited usage.

config plan-info

Parameter	Description	Type	Size	Default
currency	Currency code.	string	Maximum length: 3	
info-file	Info file.	string	Maximum length: 255	
lang	Language code.	string	Maximum length: 3	
name	Plan name.	string	Maximum length: 35	

config wireless-controller hotspot20 h2qp-conn-capability

Configure connection capability.

```
config wireless-controller hotspot20 h2qp-conn-capability
  Description: Configure connection capability.
  edit <name>
    set esp-port [closed|open|...]
    set ftp-port [closed|open|...]
    set http-port [closed|open|...]
    set icmp-port [closed|open|...]
    set ikev2-port [closed|open|...]
    set ikev2-xx-port [closed|open|...]
    set pptp-vpn-port [closed|open|...]
    set ssh-port [closed|open|...]
    set tls-port [closed|open|...]
    set voip-tcp-port [closed|open|...]
    set voip-udp-port [closed|open|...]
  next
end
```

config wireless-controller hotspot20 h2qp-conn-capability

Parameter	Description	Type	Size	Default
esp-port	Set ESP port service (used by IPsec VPNs) status.	option	-	unknown
		Option	Description	
		<i>closed</i>	The port is not open for communication.	
		<i>open</i>	The port is open for communication.	
		<i>unknown</i>	The port may or may not be open for communication.	

Parameter	Description	Type	Size	Default								
ftp-port	Set FTP port service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
http-port	Set HTTP port service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
icmp-port	Set ICMP port service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
ikev2-port	Set IKEv2 port service for IPsec VPN status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
ikev2-xx-port	Set UDP port 4500 (which may be used by IKEv2 for IPsec VPN) service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
name	Connection capability name.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default								
pptp-vpn-port	Set Point to Point Tunneling Protocol (PPTP) VPN port service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
ssh-port	Set SSH port service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
tls-port	Set TLS VPN (HTTPS) port service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
voip-tcp-port	Set VoIP TCP port service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											
voip-udp-port	Set VoIP UDP port service status.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>closed</i></td><td>The port is not open for communication.</td></tr><tr><td><i>open</i></td><td>The port is open for communication.</td></tr><tr><td><i>unknown</i></td><td>The port may or may not be open for communication.</td></tr></table>	Option	Description	<i>closed</i>	The port is not open for communication.	<i>open</i>	The port is open for communication.	<i>unknown</i>	The port may or may not be open for communication.			
Option	Description											
<i>closed</i>	The port is not open for communication.											
<i>open</i>	The port is open for communication.											
<i>unknown</i>	The port may or may not be open for communication.											

config wireless-controller hotspot20 h2qp-operator-name

Configure operator friendly name.

```
config wireless-controller hotspot20 h2qp-operator-name
  Description: Configure operator friendly name.
  edit <name>
    config value-list
      Description: Name list.
      edit <index>
        set lang {string}
        set value {string}
      next
    end
  next
end
```

config wireless-controller hotspot20 h2qp-operator-name

Parameter	Description	Type	Size	Default
name	Friendly name ID.	string	Maximum length: 35	

config value-list

Parameter	Description	Type	Size	Default
index	Value index.	integer	Minimum value: 1 Maximum value: 10	0
lang	Language code.	string	Maximum length: 3	eng
value	Friendly name value.	string	Maximum length: 252	

config wireless-controller hotspot20 h2qp-osu-provider

Configure online sign up (OSU) provider list.

```
config wireless-controller hotspot20 h2qp-osu-provider
  Description: Configure online sign up (OSU) provider list.
  edit <name>
    config friendly-name
```

```

        Description: OSU provider friendly name.
        edit <index>
            set friendly-name {string}
            set lang {string}
        next
    end
    set icon {string}
    set osu-method {option1}, {option2}, ...
    set osu-nai {string}
    set server-uri {string}
    config service-description
        Description: OSU service name.
        edit <service-id>
            set lang {string}
            set service-description {string}
        next
    end
next
end

```

config wireless-controller hotspot20 h2qp-osu-provider

Parameter	Description	Type	Size	Default
icon	OSU provider icon.	string	Maximum length: 35	
name	OSU provider ID.	string	Maximum length: 35	
osu-method	OSU method list.	option	-	
	Option	Description		
	<i>oma-dm</i>	OMA DM.		
	<i>soap-xml-spp</i>	SOAP XML SPP.		
	<i>reserved</i>	Reserved.		
osu-nai	OSU NAI.	string	Maximum length: 255	
server-uri	Server URI.	string	Maximum length: 255	

config friendly-name

Parameter	Description	Type	Size	Default
friendly-name	OSU provider friendly name.	string	Maximum length: 252	
index	OSU provider friendly name index.	integer	Minimum value: 1 Maximum value: 10	0
lang	Language code.	string	Maximum length: 3	eng

config service-description

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
service-description	Service description.	string	Maximum length: 252	
service-id	OSU service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config wireless-controller hotspot20 h2qp-osu-provider-nai

Configure online sign up (OSU) provider NAI list.

```
config wireless-controller hotspot20 h2qp-osu-provider-nai
  Description: Configure online sign up (OSU) provider NAI list.
  edit <name>
    config nai-list
      Description: OSU NAI list.
      edit <name>
        set osu-nai {string}
      next
    end
  next
end
```

config wireless-controller hotspot20 h2qp-osu-provider-nai

Parameter	Description	Type	Size	Default
name	OSU provider NAI ID.	string	Maximum length: 35	

config nai-list

Parameter	Description	Type	Size	Default
name	OSU NAI ID.	string	Maximum length: 35	
osu-nai	OSU NAI.	string	Maximum length: 255	

config wireless-controller hotspot20 h2qp-terms-and-conditions

Configure terms and conditions.

```
config wireless-controller hotspot20 h2qp-terms-and-conditions
  Description: Configure terms and conditions.
  edit <name>
    set filename {string}
    set timestamp {integer}
    set url {string}
  next
end
```

config wireless-controller hotspot20 h2qp-terms-and-conditions

Parameter	Description	Type	Size	Default
filename	Filename.	string	Maximum length: 254	
name	Terms and Conditions ID.	string	Maximum length: 35	
timestamp	Timestamp.	integer	Minimum value: 0 Maximum value: 4294967295	
url	URL.	string	Maximum length: 253	

config wireless-controller hotspot20 h2qp-wan-metric

Configure WAN metrics.

```
config wireless-controller hotspot20 h2qp-wan-metric
  Description: Configure WAN metrics.
  edit <name>
    set downlink-load {integer}
    set downlink-speed {integer}
    set link-at-capacity [enable|disable]
    set link-status [up|down|...]
    set load-measurement-duration {integer}
    set symmetric-wan-link [symmetric|asymmetric]
    set uplink-load {integer}
    set uplink-speed {integer}
  next
end
```

config wireless-controller hotspot20 h2qp-wan-metric

Parameter	Description	Type	Size	Default								
downlink-load	Downlink load.	integer	Minimum value: 0 0 Maximum value: 255	0								
downlink-speed	Downlink speed (in kilobits/s).	integer	Minimum value: 0 0 Maximum value: 4294967295	2400								
link-at-capacity	Link at capacity.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Link at capacity (not allow additional mobile devices to associate).</td></tr><tr><td><i>disable</i></td><td>Link not at capacity (allow additional mobile devices to associate).</td></tr></table>	Option	Description	<i>enable</i>	Link at capacity (not allow additional mobile devices to associate).	<i>disable</i>	Link not at capacity (allow additional mobile devices to associate).					
Option	Description											
<i>enable</i>	Link at capacity (not allow additional mobile devices to associate).											
<i>disable</i>	Link not at capacity (allow additional mobile devices to associate).											
link-status	Link status.	option	-	up								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>up</i></td><td>Link up.</td></tr><tr><td><i>down</i></td><td>Link down.</td></tr><tr><td><i>in-test</i></td><td>Link in test state.</td></tr></table>	Option	Description	<i>up</i>	Link up.	<i>down</i>	Link down.	<i>in-test</i>	Link in test state.			
Option	Description											
<i>up</i>	Link up.											
<i>down</i>	Link down.											
<i>in-test</i>	Link in test state.											

Parameter	Description	Type	Size	Default						
load-measurement-duration	Load measurement duration (in tenths of a second).	integer	Minimum value: 0 0 Maximum value: 65535	0						
name	WAN metric name.	string	Maximum length: 35							
symmetric-wan-link	WAN link symmetry.	option	-	asymmetric						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>symmetric</i></td><td>Symmetric WAN link (uplink and downlink speeds are the same).</td></tr><tr><td><i>asymmetric</i></td><td>Asymmetric WAN link (uplink and downlink speeds are not the same).</td></tr></table>				Option	Description	<i>symmetric</i>	Symmetric WAN link (uplink and downlink speeds are the same).	<i>asymmetric</i>	Asymmetric WAN link (uplink and downlink speeds are not the same).
Option	Description									
<i>symmetric</i>	Symmetric WAN link (uplink and downlink speeds are the same).									
<i>asymmetric</i>	Asymmetric WAN link (uplink and downlink speeds are not the same).									
uplink-load	Uplink load.	integer	Minimum value: 0 0 Maximum value: 255	0						
uplink-speed	Uplink speed (in kilobits/s).	integer	Minimum value: 0 0 Maximum value: 4294967295	2400						

config wireless-controller hotspot20 hs-profile

Configure hotspot profile.

```

config wireless-controller hotspot20 hs-profile
  Description: Configure hotspot profile.
  edit <name>
    set 3gpp-plmn {string}
    set access-network-asra [enable|disable]
    set access-network-esr [enable|disable]
    set access-network-internet [enable|disable]
    set access-network-type [private-network|private-network-with-guest-access|...]
    set access-network-uesa [enable|disable]
    set advice-of-charge {string}
    set anqp-domain-id {integer}
    set bss-transition [enable|disable]
    set conn-cap {string}
    set deauth-request-timeout {integer}
    set dgaf [enable|disable]
    set domain-name {string}
    set gas-comeback-delay {integer}
    set gas-fragmentation-limit {integer}
    set hessid {mac-address}
    set ip-addr-type {string}
    set l2tif [enable|disable]

```

```

set nai-realm {string}
set network-auth {string}
set oper-friendly-name {string}
set oper-icon {string}
set osu-provider <name1>, <name2>, ...
set osu-provider-nai {string}
set osu-ssid {string}
set pame-bi [disable|enable]
set proxy-arp [enable|disable]
set qos-map {string}
set release {integer}
set roaming-consortium {string}
set terms-and-conditions {string}
set venue-group [unspecified|assembly|...]
set venue-name {string}
set venue-type [unspecified|arena|...]
set venue-url {string}
set wan-metrics {string}
set wba-charging-currency {string}
set wba-charging-rate {integer}
set wba-data-clearing-provider {string}
set wba-financial-clearing-provider {string}
set wba-open-roaming [disable|enable]
set wnm-sleep-mode [enable|disable]

next
end

```

config wireless-controller hotspot20 hs-profile

Parameter	Description	Type	Size	Default						
3gpp-plmn	3GPP PLMN name.	string	Maximum length: 35							
access-network-asra	Enable/disable additional step required for access (ASRA).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable additional step required for access (ASRA).</td></tr><tr><td><i>disable</i></td><td>Disable additional step required for access (ASRA).</td></tr></table>	Option	Description	<i>enable</i>	Enable additional step required for access (ASRA).	<i>disable</i>	Disable additional step required for access (ASRA).			
Option	Description									
<i>enable</i>	Enable additional step required for access (ASRA).									
<i>disable</i>	Disable additional step required for access (ASRA).									
access-network-esr	Enable/disable emergency services reachable (ESR).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable emergency services reachable (ESR).</td></tr><tr><td><i>disable</i></td><td>Disable emergency services reachable (ESR).</td></tr></table>	Option	Description	<i>enable</i>	Enable emergency services reachable (ESR).	<i>disable</i>	Disable emergency services reachable (ESR).			
Option	Description									
<i>enable</i>	Enable emergency services reachable (ESR).									
<i>disable</i>	Disable emergency services reachable (ESR).									

Parameter	Description	Type	Size	Default																		
access-network-internet	Enable/disable connectivity to the Internet.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable connectivity to the Internet.</td></tr><tr><td><i>disable</i></td><td>Disable connectivity to the Internet.</td></tr></table>	Option	Description	<i>enable</i>	Enable connectivity to the Internet.	<i>disable</i>	Disable connectivity to the Internet.															
Option	Description																					
<i>enable</i>	Enable connectivity to the Internet.																					
<i>disable</i>	Disable connectivity to the Internet.																					
access-network-type	Access network type.	option	-	private-network																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>private-network</i></td><td>Private network.</td></tr><tr><td><i>private-network-with-guest-access</i></td><td>Private network with guest access.</td></tr><tr><td><i>chargeable-public-network</i></td><td>Chargeable public network.</td></tr><tr><td><i>free-public-network</i></td><td>Free public network.</td></tr><tr><td><i>personal-device-network</i></td><td>Personal devices network.</td></tr><tr><td><i>emergency-services-only-network</i></td><td>Emergency services only network.</td></tr><tr><td><i>test-or-experimental</i></td><td>Test or experimental.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard.</td></tr></table>	Option	Description	<i>private-network</i>	Private network.	<i>private-network-with-guest-access</i>	Private network with guest access.	<i>chargeable-public-network</i>	Chargeable public network.	<i>free-public-network</i>	Free public network.	<i>personal-device-network</i>	Personal devices network.	<i>emergency-services-only-network</i>	Emergency services only network.	<i>test-or-experimental</i>	Test or experimental.	<i>wildcard</i>	Wildcard.			
Option	Description																					
<i>private-network</i>	Private network.																					
<i>private-network-with-guest-access</i>	Private network with guest access.																					
<i>chargeable-public-network</i>	Chargeable public network.																					
<i>free-public-network</i>	Free public network.																					
<i>personal-device-network</i>	Personal devices network.																					
<i>emergency-services-only-network</i>	Emergency services only network.																					
<i>test-or-experimental</i>	Test or experimental.																					
<i>wildcard</i>	Wildcard.																					
access-network-uesa	Enable/disable unauthenticated emergency service accessible (UESA).	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unauthenticated emergency service accessible (UESA).</td></tr><tr><td><i>disable</i></td><td>Disable unauthenticated emergency service accessible (UESA).</td></tr></table>	Option	Description	<i>enable</i>	Enable unauthenticated emergency service accessible (UESA).	<i>disable</i>	Disable unauthenticated emergency service accessible (UESA).															
Option	Description																					
<i>enable</i>	Enable unauthenticated emergency service accessible (UESA).																					
<i>disable</i>	Disable unauthenticated emergency service accessible (UESA).																					
advice-of-charge	Advice of charge.	string	Maximum length: 35																			

Parameter	Description	Type	Size	Default
anqp-domain-id	ANQP Domain ID (0-65535).	integer	Minimum value: 0 0 Maximum value: 65535	0
bss-transition	Enable/disable basic service set (BSS) transition Support.	option	-	disable
	Option	Description		
	enable	Enable basic service set (BSS) transition support.		
	disable	Disable basic service set (BSS) transition support.		
conn-cap	Connection capability name.	string	Maximum length: 35	
deauth-request- timeout	Deauthentication request timeout (in seconds).	integer	Minimum value: 30 Maximum value: 120	60
dgaf	Enable/disable downstream group-addressed forwarding (DGAF).	option	-	disable
	Option	Description		
	enable	Enable downstream group-addressed forwarding (DGAF).		
	disable	Disable downstream group-addressed forwarding (DGAF).		
domain-name	Domain name.	string	Maximum length: 255	
gas-comeback- delay	GAS comeback delay (0 or 100 - 10000 milliseconds, default = 500).	integer	Minimum value: 100 Maximum value: 10000	500
gas- fragmentation- limit	GAS fragmentation limit (512 - 4096, default = 1024).	integer	Minimum value: 512 Maximum value: 4096	1024
hessid	Homogeneous extended service set identifier (HESSID).	mac- address	Not Specified	00:00:00:00:00:00
ip-addr-type	IP address type name.	string	Maximum length: 35	
l2tif	Enable/disable Layer 2 traffic inspection and filtering.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Layer 2 traffic inspection and filtering.		
	<i>disable</i>	Disable Layer 2 traffic inspection and filtering.		
nai-realm	NAI realm list name.	string	Maximum length: 35	
name	Hotspot profile name.	string	Maximum length: 35	
network-auth	Network authentication name.	string	Maximum length: 35	
oper-friendly-name	Operator friendly name.	string	Maximum length: 35	
oper-icon	Operator icon.	string	Maximum length: 35	
osu-provider <name>	Manually selected list of OSU provider(s). OSU provider name.	string	Maximum length: 35	
osu-provider-nai	OSU Provider NAI.	string	Maximum length: 35	
osu-ssid	Online sign up (OSU) SSID.	string	Maximum length: 255	
pame-bi	Enable/disable Pre-Association Message Exchange BSSID Independent (PAME-BI).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).		
	<i>enable</i>	Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).		
proxy-arp	Enable/disable Proxy ARP.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Proxy ARP.		
	<i>disable</i>	Disable Proxy ARP.		
qos-map	QoS MAP set ID.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
release	Hotspot 2.0 Release number (1, 2, 3, default = 2).	integer	Minimum value: 2 1 Maximum value: 3	
roaming-consortium	Roaming consortium list name.	string	Maximum length: 35	
terms-and-conditions	Terms and conditions.	string	Maximum length: 35	
venue-group	Venue group.	option	-	unspecified
	Option		Description	
	<i>unspecified</i>	Unspecified.		
	<i>assembly</i>	Assembly.		
	<i>business</i>	Business.		
	<i>educational</i>	Educational.		
	<i>factory</i>	Factory and industrial.		
	<i>institutional</i>	Institutional.		
	<i>mercantile</i>	Mercantile.		
	<i>residential</i>	Residential.		
	<i>storage</i>	Storage.		
	<i>utility</i>	Utility and miscellaneous.		
	<i>vehicular</i>	Vehicular.		
	<i>outdoor</i>	Outdoor.		
venue-name	Venue name.	string	Maximum length: 35	
venue-type	Venue type.	option	-	unspecified
	Option		Description	
	<i>unspecified</i>	Unspecified.		
	<i>arena</i>	Arena.		
	<i>stadium</i>	Stadium.		
	<i>passenger-terminal</i>	Passenger terminal.		
	<i>amphitheater</i>	Amphitheater.		
	<i>amusement-park</i>	Amusement park.		

Parameter	Description	Type	Size	Default

Option	Description
<i>place-of-worship</i>	Place of worship.
<i>convention-center</i>	Convention center.
<i>library</i>	Library.
<i>museum</i>	Museum.
<i>restaurant</i>	Restaurant.
<i>theater</i>	Theater.
<i>bar</i>	Bar.
<i>coffee-shop</i>	Coffee shop.
<i>zoo-or-aquarium</i>	Zoo or aquarium.
<i>emergency-center</i>	Emergency coordination center.
<i>doctor-office</i>	Doctor or dentist office.
<i>bank</i>	Bank.
<i>fire-station</i>	Fire station.
<i>police-station</i>	Police station.
<i>post-office</i>	Post office.
<i>professional-office</i>	Professional office.
<i>research-facility</i>	Research and development facility.
<i>attorney-office</i>	Attorney office.
<i>primary-school</i>	Primary school.
<i>secondary-school</i>	Secondary school.
<i>university-or-college</i>	University or college.
<i>factory</i>	Factory.
<i>hospital</i>	Hospital.
<i>long-term-care-facility</i>	Long term care facility.
<i>rehab-center</i>	Alcohol and drug rehabilitation center.
<i>group-home</i>	Group home.
<i>prison-or-jail</i>	Prison or jail.
<i>retail-store</i>	Retail store.
<i>grocery-market</i>	Grocery market.

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto-service-station</i>	Auto service station.		
	<i>shopping-mall</i>	Shopping mall.		
	<i>gas-station</i>	Gas station.		
	<i>private</i>	Private residence.		
	<i>hotel-or-motel</i>	Hotel or motel.		
	<i>dormitory</i>	Dormitory.		
	<i>boarding-house</i>	Boarding house.		
	<i>automobile</i>	Automobile or truck.		
	<i>airplane</i>	Airplane.		
	<i>bus</i>	Bus.		
	<i>ferry</i>	Ferry.		
	<i>ship-or-boat</i>	Ship or boat.		
	<i>train</i>	Train.		
	<i>motor-bike</i>	Motor bike.		
	<i>muni-mesh-network</i>	Muni mesh network.		
	<i>city-park</i>	City park.		
	<i>rest-area</i>	Rest area.		
	<i>traffic-control</i>	Traffic control.		
	<i>bus-stop</i>	Bus stop.		
	<i>kiosk</i>	Kiosk.		
venue-url	Venue name.	string	Maximum length: 35	
wan-metrics	WAN metric name.	string	Maximum length: 35	
wba-charging-currency	Three letter currency code.	string	Maximum length: 3	
wba-charging-rate	Number of currency units per kilobyte.	integer	Minimum value: 0 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default						
wba-data-clearing-provider	WBA ID of data clearing provider.	string	Maximum length: 127							
wba-financial-clearing-provider	WBA ID of financial clearing provider.	string	Maximum length: 127							
wba-open-roaming	Enable/disable WBA open roaming support.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable WBA open roaming support.</td></tr><tr><td>enable</td><td>Enable WBA open roaming support.</td></tr></table>				Option	Description	disable	Disable WBA open roaming support.	enable	Enable WBA open roaming support.
Option	Description									
disable	Disable WBA open roaming support.									
enable	Enable WBA open roaming support.									
wnm-sleep-mode	Enable/disable wireless network management (WNM) sleep mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable wireless network management (WNM) sleep mode.</td></tr><tr><td>disable</td><td>Disable wireless network management (WNM) sleep mode.</td></tr></table>				Option	Description	enable	Enable wireless network management (WNM) sleep mode.	disable	Disable wireless network management (WNM) sleep mode.
Option	Description									
enable	Enable wireless network management (WNM) sleep mode.									
disable	Disable wireless network management (WNM) sleep mode.									

config wireless-controller hotspot20 icon

Configure OSU provider icon.

```

config wireless-controller hotspot20 icon
  Description: Configure OSU provider icon.
  edit <name>
    config icon-list
      Description: Icon list.
      edit <name>
        set file {string}
        set height {integer}
        set lang {string}
        set type [bmp|gif|...]
        set width {integer}
      next
    end
  next
end

```

config wireless-controller hotspot20 icon

Parameter	Description	Type	Size	Default
name	Icon list ID.	string	Maximum length: 35	

config icon-list

Parameter	Description	Type	Size	Default
file	Icon file.	string	Maximum length: 255	
height	Icon height.	integer	Minimum value: 1 Maximum value: 65535	0
lang	Language code.	string	Maximum length: 3	eng
name	Icon name.	string	Maximum length: 255	
type	Icon type.	option	-	png
	Option Description			
	bmp BMP image.			
	gif GIF image.			
	jpeg JPEG image.			
	png PNG image.			
	tiff TIFF image.			
width	Icon width.	integer	Minimum value: 1 Maximum value: 65535	0

config wireless-controller hotspot20 qos-map

Configure QoS map set.

```

config wireless-controller hotspot20 qos-map
  Description: Configure QoS map set.
  edit <name>
    config dscp-except
      Description: Differentiated Services Code Point (DSCP) exceptions.
      edit <index>
        set dscp {integer}
        set up {integer}
      next
    end
  config dscp-range
    Description: Differentiated Services Code Point (DSCP) ranges.
    edit <index>
      set high {integer}
      set low {integer}
      set up {integer}
    next
  end
next
end

```

config wireless-controller hotspot20 qos-map

Parameter	Description	Type	Size	Default
name	QOS-MAP name.	string	Maximum length: 35	

config dscp-except

Parameter	Description	Type	Size	Default
dscp	DSCP value.	integer	Minimum value: 0 Maximum value: 63	0
index	DSCP exception index.	integer	Minimum value: 1 Maximum value: 21	0
up	User priority.	integer	Minimum value: 0 Maximum value: 7	0

config dscp-range

Parameter	Description	Type	Size	Default
high	DSCP high value.	integer	Minimum value: 0 Maximum value: 63	255
index	DSCP range index.	integer	Minimum value: 1 Maximum value: 8	0
low	DSCP low value.	integer	Minimum value: 0 Maximum value: 63	255
up	User priority.	integer	Minimum value: 0 Maximum value: 7	0

config wireless-controller inter-controller

Configure inter wireless controller operation.

```
config wireless-controller inter-controller
  Description: Configure inter wireless controller operation.
  set fast-failover-max {integer}
  set fast-failover-wait {integer}
  set inter-controller-key {password}
  set inter-controller-mode [disable|l2-roaming|...]
  config inter-controller-peer
    Description: Fast failover peer wireless controller list.
    edit <id>
      set peer-ip {ipv4-address}
      set peer-port {integer}
      set peer-priority [primary|secondary]
    next
  end
  set inter-controller-pri [primary|secondary]
  set l3-roaming [enable|disable]
end
```

config wireless-controller inter-controller

Parameter	Description	Type	Size	Default								
fast-failover-max	Maximum number of retransmissions for fast failover HA messages between peer wireless controllers (3 - 64, default = 10).	integer	Minimum value: 3 Maximum value: 64	10								
fast-failover-wait	Minimum wait time before an AP transitions from secondary controller to primary controller (10 - 86400 sec, default = 10).	integer	Minimum value: 10 Maximum value: 86400	10								
inter-controller-key	Secret key for inter-controller communications.	password	Not Specified									
inter-controller-mode	Configure inter-controller mode (disable, l2-roaming, 1+1, default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable inter-controller mode.</td></tr><tr><td>l2-roaming</td><td>Enable layer 2 roaming support between inter-controllers.</td></tr><tr><td>1+1</td><td>Enable 1+1 fast failover mode.</td></tr></table>	Option	Description	disable	Disable inter-controller mode.	l2-roaming	Enable layer 2 roaming support between inter-controllers.	1+1	Enable 1+1 fast failover mode.			
Option	Description											
disable	Disable inter-controller mode.											
l2-roaming	Enable layer 2 roaming support between inter-controllers.											
1+1	Enable 1+1 fast failover mode.											
inter-controller-pri	Configure inter-controller's priority (primary or secondary, default = primary).	option	-	primary								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>primary</td><td>Primary fast failover mode.</td></tr><tr><td>secondary</td><td>Secondary fast failover mode.</td></tr></table>	Option	Description	primary	Primary fast failover mode.	secondary	Secondary fast failover mode.					
Option	Description											
primary	Primary fast failover mode.											
secondary	Secondary fast failover mode.											
l3-roaming	Enable/disable layer 3 roaming (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable layer 3 roaming.</td></tr><tr><td>disable</td><td>Disable layer 3 roaming.</td></tr></table>	Option	Description	enable	Enable layer 3 roaming.	disable	Disable layer 3 roaming.					
Option	Description											
enable	Enable layer 3 roaming.											
disable	Disable layer 3 roaming.											

config inter-controller-peer

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
peer-ip	Peer wireless controller's IP address.	ipv4-address	Not Specified	0.0.0.0
peer-port	Port used by the wireless controller's for inter-controller communications (1024 - 49150, default = 5246).	integer	Minimum value: 1024 Maximum value: 49150	5246
peer-priority	Peer wireless controller's priority (primary or secondary, default = primary).	option	-	primary
		Option	Description	
		primary	Primary fast failover mode.	
		secondary	Secondary fast failover mode.	

config wireless-controller log

Configure wireless controller event log filters.

```
config wireless-controller log
  Description: Configure wireless controller event log filters.
  set addrgrp-log [emergency|alert|...]
  set ble-log [emergency|alert|...]
  set clb-log [emergency|alert|...]
  set dhcp-starv-log [emergency|alert|...]
  set led-sched-log [emergency|alert|...]
  set radio-event-log [emergency|alert|...]
  set rogue-event-log [emergency|alert|...]
  set sta-event-log [emergency|alert|...]
  set sta-locate-log [emergency|alert|...]
  set status [enable|disable]
  set wids-log [emergency|alert|...]
  set wtp-event-log [emergency|alert|...]
  set wtp-fips-event-log [emergency|alert|...]
end
```

config wireless-controller log

Parameter	Description	Type	Size	Default
addrgrp-log	Lowest severity level to log address group message.	option	-	notification
		Option	Description	
		<i>emergency</i>	Emergency level.	
		<i>alert</i>	Alert level.	
		<i>critical</i>	Critical level.	
		<i>error</i>	Error level.	
		<i>warning</i>	Warning level.	
		<i>notification</i>	Notification level.	
		<i>information</i>	Information level.	
		<i>debug</i>	Debug level.	
ble-log	Lowest severity level to log BLE detection message.	option	-	notification
		Option	Description	
		<i>emergency</i>	Emergency level.	
		<i>alert</i>	Alert level.	
		<i>critical</i>	Critical level.	
		<i>error</i>	Error level.	
		<i>warning</i>	Warning level.	
		<i>notification</i>	Notification level.	
		<i>information</i>	Information level.	
		<i>debug</i>	Debug level.	
clb-log	Lowest severity level to log client load balancing message.	option	-	notification
		Option	Description	
		<i>emergency</i>	Emergency level.	
		<i>alert</i>	Alert level.	
		<i>critical</i>	Critical level.	

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.									
	Option	Description																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
	<i>debug</i>	Debug level.																				
dhcp-starv-log	Lowest severity level to log DHCP starvation event message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
led-sched-log	Lowest severity level to log LED schedule event message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
radio-event-log	Lowest severity level to log radio event message.	option	-	notification																		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
rogue-event-log	Lowest severity level to log rogue AP event message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
sta-event-log	Lowest severity level to log station event message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.							
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
<i>notification</i>	Notification level.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sta-locate-log	Lowest severity level to log station locate message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
status	Enable/disable wireless event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable wireless event logging.		
	<i>disable</i>	Disable wireless event logging.		
wids-log	Lowest severity level to log WIDS message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		

Parameter	Description	Type	Size	Default
wtp-event-log	Lowest severity level to log WTP event message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
wtp-fips-event-log	Lowest severity level to log FAP fips event message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		

config wireless-controller mpsk-profile

Configure MPSK profile.

```
config wireless-controller mpsk-profile
  Description: Configure MPSK profile.
  edit <name>
    set mpsk-concurrent-clients {integer}
    set mpsk-external-server {string}
    set mpsk-external-server-auth [enable|disable]
  config mpsk-group
    Description: List of multiple PSK groups.
```

```

edit <name>
  config mpsk-key
    Description: List of multiple PSK entries.
    edit <name>
      set comment {var-string}
      set concurrent-client-limit-type [default|unlimited|...]
      set concurrent-clients {integer}
      set key-type [wpa2-personal|wpa3-sae]
      set mac {mac-address}
      set mpsk-schedules <name1>, <name2>, ...
      set passphrase {password}
      set sae-password {password}
      set sae-pk [enable|disable]
      set sae-private-key {string}
    next
  end
  set vlan-id {integer}
  set vlan-type [no-vlan|fixed-vlan]
next
end
set mpsk-type [wpa2-personal|wpa3-sae|...]
next
end

```

config wireless-controller mpsk-profile

Parameter	Description	Type	Size	Default						
mpsk-concurrent-clients	Maximum number of concurrent clients that connect using the same passphrase in multiple PSK authentication (0 - 65535, default = 0, meaning no limitation).	integer	Minimum value: 0 Maximum value: 65535	0						
mpsk-external-server	RADIUS server to be used to authenticate MPSK users.	string	Maximum length: 35							
mpsk-external-server-auth	Enable/Disable MPSK external server authentication (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MPSK external server authentication.</td></tr><tr><td><i>disable</i></td><td>Disable MPSK external server authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable MPSK external server authentication.	<i>disable</i>	Disable MPSK external server authentication.
Option	Description									
<i>enable</i>	Enable MPSK external server authentication.									
<i>disable</i>	Disable MPSK external server authentication.									
mpsk-type	Select the security type of keys for this profile.	option	-	wpa2-personal						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wpa2-personal</i>	WPA2 personal.		
	<i>wpa3-sae</i>	WPA3 SAE.		
	<i>wpa3-sae-transition</i>	WPA3 SAE transition.		
name	MPSK profile name.	string	Maximum length: 35	

config mpsk-group

Parameter	Description	Type	Size	Default
name	MPSK group name.	string	Maximum length: 35	
vlan-id	Optional VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0
vlan-type	MPSK group VLAN options.	option	-	no-vlan
	Option	Description		
	<i>no-vlan</i>	No VLAN.		
	<i>fixed-vlan</i>	Fixed VLAN ID.		

config mpsk-key

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
concurrent-client-limit-type	MPSK client limit type options.	option	-	default
	Option	Description		
	<i>default</i>	Using the value in profile configuration.		
	<i>unlimited</i>	Unlimited.		
	<i>specified</i>	Specified value.		

Parameter	Description	Type	Size	Default						
concurrent-clients	Number of clients that can connect using this pre-shared key (1 - 65535, default is 256).	integer	Minimum value: 1 Maximum value: 65535	256						
key-type	Select the type of the key.	option	-	wpa2-personal						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wpa2-personal</td><td>WPA2 personal.</td></tr><tr><td>wpa3-sae</td><td>WPA3 SAE.</td></tr></table>	Option	Description	wpa2-personal	WPA2 personal.	wpa3-sae	WPA3 SAE.			
Option	Description									
wpa2-personal	WPA2 personal.									
wpa3-sae	WPA3 SAE.									
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00						
mpsk-schedules <name>	Firewall schedule for MPSK passphrase. The passphrase will be effective only when at least one schedule is valid. Schedule name.	string	Maximum length: 35							
name	Pre-shared key name.	string	Maximum length: 35							
passphrase	WPA Pre-shared key.	password	Not Specified							
sae-password	WPA3 SAE password.	password	Not Specified							
sae-pk	Enable/disable WPA3 SAE-PK (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WPA3 SAE-PK.</td></tr><tr><td>disable</td><td>Disable WPA3 SAE-PK.</td></tr></table>	Option	Description	enable	Enable WPA3 SAE-PK.	disable	Disable WPA3 SAE-PK.			
Option	Description									
enable	Enable WPA3 SAE-PK.									
disable	Disable WPA3 SAE-PK.									
sae-private-key	Private key used for WPA3 SAE-PK authentication.	string	Maximum length: 359							

config wireless-controller nac-profile

Configure WiFi network access control (NAC) profiles.

```
config wireless-controller nac-profile
  Description: Configure WiFi network access control (NAC) profiles.
  edit <name>
    set comment {var-string}
```

```

        set onboarding-vlan {string}
    next
end

```

config wireless-controller nac-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Name.	string	Maximum length: 35	
onboarding-vlan	VLAN interface name.	string	Maximum length: 35	

config wireless-controller qos-profile

Configure WiFi quality of service (QoS) profiles.

```

config wireless-controller qos-profile
    Description: Configure WiFi quality of service (QoS) profiles.
    edit <name>
        set bandwidth-admission-control [enable|disable]
        set bandwidth-capacity {integer}
        set burst [enable|disable]
        set call-admission-control [enable|disable]
        set call-capacity {integer}
        set comment {string}
        set downlink {integer}
        set downlink-sta {integer}
        set dscp-wmm-be <id1>, <id2>, ...
        set dscp-wmm-bk <id1>, <id2>, ...
        set dscp-wmm-mapping [enable|disable]
        set dscp-wmm-vi <id1>, <id2>, ...
        set dscp-wmm-vo <id1>, <id2>, ...
        set uplink {integer}
        set uplink-sta {integer}
        set wmm [enable|disable]
        set wmm-be-dscp {integer}
        set wmm-bk-dscp {integer}
        set wmm-dscp-marking [enable|disable]
        set wmm-uapsd [enable|disable]
        set wmm-vi-dscp {integer}
        set wmm-vo-dscp {integer}
    next
end

```


config wireless-controller qos-profile

Parameter	Description	Type	Size	Default						
bandwidth-admission-control	Enable/disable WMM bandwidth admission control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 1 Maximum value: 600000	2000						
burst	Enable/disable client rate burst.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable client rate burst.</td></tr><tr><td><i>disable</i></td><td>Disable client rate burst.</td></tr></table>	Option	Description	<i>enable</i>	Enable client rate burst.	<i>disable</i>	Disable client rate burst.			
Option	Description									
<i>enable</i>	Enable client rate burst.									
<i>disable</i>	Disable client rate burst.									
call-admission-control	Enable/disable WMM call admission control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.			
Option	Description									
<i>enable</i>	Enable WMM call admission control.									
<i>disable</i>	Disable WMM call admission control.									
call-capacity	Maximum number of Voice over WLAN (VoWLAN) phones allowed (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60	10						
comment	Comment.	string	Maximum length: 63							
downlink	Maximum downlink bandwidth for Virtual Access Points (VAPs) (0 - 2097152 Kbps, default = 0, 0 means no limit).	integer	Minimum value: 0 Maximum value: 2097152	0						

Parameter	Description	Type	Size	Default						
downlink-sta	Maximum downlink bandwidth for clients (0 - 2097152 Kbps, default = 0, 0 means no limit).	integer	Minimum value: 0 Maximum value: 2097152	0						
dscp-wmm-be <id>	DSCP mapping for best effort access (default = 0 24). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
dscp-wmm-bk <id>	DSCP mapping for background access (default = 8 16). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
dscp-wmm-mapping	Enable/disable Differentiated Services Code Point (DSCP) mapping.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Differentiated Services Code Point (DSCP) mapping.</td></tr><tr><td>disable</td><td>Disable Differentiated Services Code Point (DSCP) mapping.</td></tr></table>				Option	Description	enable	Enable Differentiated Services Code Point (DSCP) mapping.	disable	Disable Differentiated Services Code Point (DSCP) mapping.
Option	Description									
enable	Enable Differentiated Services Code Point (DSCP) mapping.									
disable	Disable Differentiated Services Code Point (DSCP) mapping.									
dscp-wmm-vi <id>	DSCP mapping for video access (default = 32 40). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
dscp-wmm-vo <id>	DSCP mapping for voice access (default = 48 56). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
name	WiFi QoS profile name.	string	Maximum length: 35							
uplink	Maximum uplink bandwidth for Virtual Access Points (VAPs) (0 - 2097152 Kbps, default = 0, 0 means no limit).	integer	Minimum value: 0 Maximum value: 2097152	0						
uplink-sta	Maximum uplink bandwidth for clients (0 - 2097152 Kbps, default = 0, 0 means no limit).	integer	Minimum value: 0 Maximum value: 2097152	0						
wmm	Enable/disable WiFi multi-media (WMM) control.	option	-	enable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiFi multi-media (WMM) control.</td></tr><tr><td><i>disable</i></td><td>Disable WiFi multi-media (WMM) control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WiFi multi-media (WMM) control.	<i>disable</i>	Disable WiFi multi-media (WMM) control.			
Option	Description									
<i>enable</i>	Enable WiFi multi-media (WMM) control.									
<i>disable</i>	Disable WiFi multi-media (WMM) control.									
wmm-be-dscp	DSCP marking for best effort access (default = 0).	integer	Minimum value: 0 Maximum value: 63	0						
wmm-bk-dscp	DSCP marking for background access (default = 8).	integer	Minimum value: 0 Maximum value: 63	8						
wmm-dscp-marking	Enable/disable WMM Differentiated Services Code Point (DSCP) marking.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM Differentiated Services Code Point (DSCP) marking.</td></tr><tr><td><i>disable</i></td><td>Disable WMM Differentiated Services Code Point (DSCP) marking.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM Differentiated Services Code Point (DSCP) marking.	<i>disable</i>	Disable WMM Differentiated Services Code Point (DSCP) marking.			
Option	Description									
<i>enable</i>	Enable WMM Differentiated Services Code Point (DSCP) marking.									
<i>disable</i>	Disable WMM Differentiated Services Code Point (DSCP) marking.									
wmm-uapsd	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.</td></tr><tr><td><i>disable</i></td><td>Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	<i>disable</i>	Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.			
Option	Description									
<i>enable</i>	Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.									
<i>disable</i>	Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.									
wmm-vi-dscp	DSCP marking for video access (default = 32).	integer	Minimum value: 0 Maximum value: 63	32						
wmm-vo-dscp	DSCP marking for voice access (default = 48).	integer	Minimum value: 0 Maximum value: 63	48						

config wireless-controller region

Configure FortiAP regions (for floor plans and maps).

```

config wireless-controller region
  Description: Configure FortiAP regions (for floor plans and maps).
  edit <name>
    set comments {string}
    set grayscale [enable|disable]
    set opacity {integer}
  next
end

```

config wireless-controller region

Parameter	Description	Type	Size	Default						
comments	Comments.	string	Maximum length: 1027							
grayscale	Region image grayscale.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable region image grayscale.</td></tr><tr><td><i>disable</i></td><td>Disable region image grayscale.</td></tr></table>				Option	Description	<i>enable</i>	Enable region image grayscale.	<i>disable</i>	Disable region image grayscale.
	Option	Description								
	<i>enable</i>	Enable region image grayscale.								
<i>disable</i>	Disable region image grayscale.									
name	FortiAP region name.	string	Maximum length: 35							
opacity	Region image opacity (0 - 100).	integer	Minimum value: 0 Maximum value: 100	100						

config wireless-controller setting

VDOM wireless controller configuration.

```

config wireless-controller setting
  Description: VDOM wireless controller configuration.
  set account-id {string}
  set country [--|AF|...]
  set darrp-optimize {integer}
  set darrp-optimize-schedules <name1>, <name2>, ...
  set device-holdoff {integer}
  set device-idle {integer}
  set device-weight {integer}
  set duplicate-ssid [enable|disable]
  set fake-ssid-action {option1}, {option2}, ...
  set fapc-compatibility [enable|disable]

```

```

set firmware-provision-on-authorization [enable|disable]
config offending-ssid
    Description: Configure offending SSID.
    edit <id>
        set action {option1}, {option2}, ...
        set ssid-pattern {string}
    next
end
set phishing-ssid-detect [enable|disable]
set rolling-wtp-upgrade [enable|disable]
set wfa-compatibility [enable|disable]
end

```

config wireless-controller setting

Parameter	Description	Type	Size	Default
account-id	FortiCloud customer account ID.	string	Maximum length: 63	
country	Country or region in which the FortiGate is located. The country determines the 802.11 bands and channels that are available.	option	-	US
	Option		Description	
	--	NO_COUNTRY_SET		
	AF	AFGHANISTAN		
	AL	ALBANIA		
	DZ	ALGERIA		
	AS	AMERICAN SAMOA		
	AO	ANGOLA		
	AR	ARGENTINA		
	AM	ARMENIA		
	AU	AUSTRALIA		
	AT	AUSTRIA		
	AZ	AZERBAIJAN		
	BS	BAHAMAS		
	BH	BAHRAIN		
	BD	BANGLADESH		
	BB	BARBADOS		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>BY</i>	BELARUS		
	<i>BE</i>	BELGIUM		
	<i>BZ</i>	BELIZE		
	<i>BJ</i>	BENIN		
	<i>BM</i>	BERMUDA		
	<i>BT</i>	BHUTAN		
	<i>BO</i>	BOLIVIA		
	<i>BA</i>	BOSNIA AND HERZEGOVINA		
	<i>BW</i>	BOTSWANA		
	<i>BR</i>	BRAZIL		
	<i>BN</i>	BRUNEI DARUSSALAM		
	<i>BG</i>	BULGARIA		
	<i>BF</i>	BURKINA-FASO		
	<i>KH</i>	CAMBODIA		
	<i>CM</i>	CAMEROON		
	<i>KY</i>	CAYMAN ISLANDS		
	<i>CF</i>	CENTRAL AFRICA REPUBLIC		
	<i>TD</i>	CHAD		
	<i>CL</i>	CHILE		
	<i>CN</i>	CHINA		
	<i>CX</i>	CHRISTMAS ISLAND		
	<i>CO</i>	COLOMBIA		
	<i>CG</i>	CONGO REPUBLIC		
	<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO		
	<i>CR</i>	COSTA RICA		
	<i>HR</i>	CROATIA		
	<i>CY</i>	CYPRUS		
	<i>CZ</i>	CZECH REPUBLIC		
	<i>DK</i>	DENMARK		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>DJ</i>	DJIBOUTI		
	<i>DM</i>	DOMINICA		
	<i>DO</i>	DOMINICAN REPUBLIC		
	<i>EC</i>	ECUADOR		
	<i>EG</i>	EGYPT		
	<i>SV</i>	EL SALVADOR		
	<i>ET</i>	ETHIOPIA		
	<i>EE</i>	ESTONIA		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		
	<i>FO</i>	FAEROE ISLANDS		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GA</i>	GABON		
	<i>GE</i>	GEORGIA		
	<i>GM</i>	GAMBIA		
	<i>DE</i>	GERMANY		
	<i>GH</i>	GHANA		
	<i>GI</i>	GIBRALTAR		
	<i>GR</i>	GREECE		
	<i>GL</i>	GREENLAND		
	<i>GD</i>	GRENADA		
	<i>GP</i>	GUADELOUPE		
	<i>GU</i>	GUAM		
	<i>GT</i>	GUATEMALA		
	<i>GY</i>	GUYANA		
	<i>HT</i>	HAITI		
	<i>HN</i>	HONDURAS		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>HK</i>	HONG KONG		
	<i>HU</i>	HUNGARY		
	<i>IS</i>	ICELAND		
	<i>IN</i>	INDIA		
	<i>ID</i>	INDONESIA		
	<i>IQ</i>	IRAQ		
	<i>IE</i>	IRELAND		
	<i>IM</i>	ISLE OF MAN		
	<i>IL</i>	ISRAEL		
	<i>IT</i>	ITALY		
	<i>CI</i>	COTE_D_IVOIRE		
	<i>JM</i>	JAMAICA		
	<i>JO</i>	JORDAN		
	<i>KZ</i>	KAZAKHSTAN		
	<i>KE</i>	KENYA		
	<i>KR</i>	KOREA REPUBLIC		
	<i>KW</i>	KUWAIT		
	<i>LA</i>	LAOS		
	<i>LV</i>	LATVIA		
	<i>LB</i>	LEBANON		
	<i>LS</i>	LESOTHO		
	<i>LR</i>	LIBERIA		
	<i>LY</i>	LIBYA		
	<i>LI</i>	LIECHTENSTEIN		
	<i>LT</i>	LITHUANIA		
	<i>LU</i>	LUXEMBOURG		
	<i>MO</i>	MACAU SAR		
	<i>MK</i>	MACEDONIA, FYRO		
	<i>MG</i>	MADAGASCAR		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>MW</i>	MALAWI		
	<i>MY</i>	MALAYSIA		
	<i>MV</i>	MALDIVES		
	<i>ML</i>	MALI		
	<i>MT</i>	MALTA		
	<i>MH</i>	MARSHALL ISLANDS		
	<i>MQ</i>	MARTINIQUE		
	<i>MR</i>	MAURITANIA		
	<i>MU</i>	MAURITIUS		
	<i>YT</i>	MAYOTTE		
	<i>MX</i>	MEXICO		
	<i>FM</i>	MICRONESIA		
	<i>MD</i>	REPUBLIC OF MOLDOVA		
	<i>MC</i>	MONACO		
	<i>MN</i>	MONGOLIA		
	<i>MA</i>	MOROCCO		
	<i>MZ</i>	MOZAMBIQUE		
	<i>MM</i>	MYANMAR		
	<i>NA</i>	NAMIBIA		
	<i>NP</i>	NEPAL		
	<i>NL</i>	NETHERLANDS		
	<i>AN</i>	NETHERLANDS ANTILLES		
	<i>AW</i>	ARUBA		
	<i>NZ</i>	NEW ZEALAND		
	<i>NI</i>	NICARAGUA		
	<i>NE</i>	NIGER		
	<i>NG</i>	NIGERIA		
	<i>NO</i>	NORWAY		
	<i>MP</i>	NORTHERN MARIANA ISLANDS		

Parameter	Description	Type	Size	Default
	Option	Description		
	OM	OMAN		
	PK	PAKISTAN		
	PW	PALAU		
	PA	PANAMA		
	PG	PAPUA NEW GUINEA		
	PY	PARAGUAY		
	PE	PERU		
	PH	PHILIPPINES		
	PL	POLAND		
	PT	PORTUGAL		
	PR	PUERTO RICO		
	QA	QATAR		
	RE	REUNION		
	RO	ROMANIA		
	RU	RUSSIA		
	RW	RWANDA		
	BL	SAINT BARTHELEMY		
	KN	SAINT KITTS AND NEVIS		
	LC	SAINT LUCIA		
	MF	SAINT MARTIN		
	PM	SAINT PIERRE AND MIQUELON		
	VC	SAINT VINCENT AND GRENADIENS		
	SA	SAUDI ARABIA		
	SN	SENEGAL		
	RS	REPUBLIC OF SERBIA		
	ME	MONTENEGRO		
	SL	SIERRA LEONE		
	SG	SINGAPORE		
	SK	SLOVAKIA		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>SI</i>	SLOVENIA		
	<i>SO</i>	SOMALIA		
	<i>ZA</i>	SOUTH AFRICA		
	<i>ES</i>	SPAIN		
	<i>LK</i>	SRI LANKA		
	<i>SR</i>	SURINAME		
	<i>SZ</i>	SWAZILAND		
	<i>SE</i>	SWEDEN		
	<i>CH</i>	SWITZERLAND		
	<i>TW</i>	TAIWAN		
	<i>TZ</i>	TANZANIA		
	<i>TH</i>	THAILAND		
	<i>TL</i>	TIMOR-LESTE		
	<i>TG</i>	TOGO		
	<i>TT</i>	TRINIDAD AND TOBAGO		
	<i>TN</i>	TUNISIA		
	<i>TR</i>	TURKEY		
	<i>TM</i>	TURKMENISTAN		
	<i>AE</i>	UNITED ARAB EMIRATES		
	<i>TC</i>	TURKS AND CAICOS		
	<i>UG</i>	UGANDA		
	<i>UA</i>	UKRAINE		
	<i>GB</i>	UNITED KINGDOM		
	<i>US</i>	UNITED STATES2		
	<i>PS</i>	UNITED STATES (PUBLIC SAFETY)		
	<i>UY</i>	URUGUAY		
	<i>UZ</i>	UZBEKISTAN		
	<i>VU</i>	VANUATU		
	<i>VE</i>	VENEZUELA		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>VN</td><td>VIET NAM</td></tr><tr><td>VI</td><td>VIRGIN ISLANDS</td></tr><tr><td>WF</td><td>WALLIS AND FUTUNA</td></tr><tr><td>YE</td><td>YEMEN</td></tr><tr><td>ZM</td><td>ZAMBIA</td></tr><tr><td>ZW</td><td>ZIMBABWE</td></tr><tr><td>JP</td><td>JAPAN14</td></tr><tr><td>CA</td><td>CANADA2</td></tr></table>	Option	Description	VN	VIET NAM	VI	VIRGIN ISLANDS	WF	WALLIS AND FUTUNA	YE	YEMEN	ZM	ZAMBIA	ZW	ZIMBABWE	JP	JAPAN14	CA	CANADA2			
	Option	Description																				
	VN	VIET NAM																				
	VI	VIRGIN ISLANDS																				
	WF	WALLIS AND FUTUNA																				
	YE	YEMEN																				
	ZM	ZAMBIA																				
	ZW	ZIMBABWE																				
	JP	JAPAN14																				
CA	CANADA2																					
darrp-optimize	Time for running Distributed Automatic Radio Resource Provisioning (DARRP) optimizations (0 - 86400 sec, default = 86400, 0 = disable).	integer	Minimum value: 0 Maximum value: 86400	86400																		
darrp-optimize-schedules <name>	Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35																			
device-holdoff	Lower limit of creation time of device for identification in minutes (0 - 60, default = 5).	integer	Minimum value: 0 Maximum value: 60	5																		
device-idle	Upper limit of idle time of device for identification in minutes (0 - 14400, default = 1440).	integer	Minimum value: 0 Maximum value: 14400	1440																		
device-weight	Upper limit of confidence of device for identification (0 - 255, default = 1, 0 = disable).	integer	Minimum value: 0 Maximum value: 255	1																		
duplicate-ssid	Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM.	option	-	disable																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Allow VAPs to use the same SSID name in the same VDOM.		
	<i>disable</i>	Do not allow VAPs to use the same SSID name in the same VDOM.		
fake-ssid-action	Actions taken for detected fake SSID.	option	-	log
	Option	Description		
	<i>log</i>	Write logs for detected fake SSID.		
	<i>suppress</i>	Suppress detected fake SSID.		
fapc-compatibility	Enable/disable FAP-C series compatibility.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FAP-C series compatibility.		
	<i>disable</i>	Disable FAP-C series compatibility.		
firmware-provision-on-authorization	Enable/disable automatic provisioning of latest firmware on authorization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable firmware provision on authorization.		
	<i>disable</i>	Disable firmware provision on authorization.		
phishing-ssid-detect	Enable/disable phishing SSID detection.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable phishing SSID detection.		
	<i>disable</i>	Disable phishing SSID detection.		
rolling-wtp-upgrade	Enable/disable rolling WTP upgrade (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable rolling WTP upgrade.		
	<i>disable</i>	Disable rolling WTP upgrade.		

Parameter	Description	Type	Size	Default
wfa-compatibility	Enable/disable WFA compatibility.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Wi-Fi Alliance Certification compatibility.		
	<i>disable</i>	Disable Wi-Fi Alliance Certification compatibility.		

config offending-ssid

Parameter	Description	Type	Size	Default
action	Actions taken for detected offending SSID.	option	-	log
	Option	Description		
	<i>log</i>	Generate logs for detected offending SSID.		
	<i>suppress</i>	Suppress detected offending SSID.		
id	ID.	integer	Minimum value: 0 Maximum value: 65535	0
ssid-pattern	Define offending SSID pattern (case insensitive). For example, word, word*, *word, wo*rd.	string	Maximum length: 33	

config wireless-controller snmp

Configure SNMP.

```

config wireless-controller snmp
  Description: Configure SNMP.
  config community
    Description: SNMP Community Configuration.
    edit <id>
      config hosts
        Description: Configure IPv4 SNMP managers (hosts).
        edit <id>
          set ip {user}
        next
      end
    set name {string}
    set query-v1-status [enable|disable]
    set query-v2c-status [enable|disable]
    set status [enable|disable]
  
```

```

        set trap-v1-status [enable|disable]
        set trap-v2c-status [enable|disable]
    next
end
set contact-info {string}
set engine-id {string}
set trap-high-cpu-threshold {integer}
set trap-high-mem-threshold {integer}
config user
    Description: SNMP User Configuration.
    edit <name>
        set auth-proto [md5|sha|...]
        set auth-pwd {password}
        set notify-hosts {ipv4-address}
        set priv-proto [aes|des|...]
        set priv-pwd {password}
        set queries [enable|disable]
        set security-level [no-auth-no-priv|auth-no-priv|...]
        set status [enable|disable]
        set trap-status [enable|disable]
    next
end
end

```

config wireless-controller snmp

Parameter	Description	Type	Size	Default
contact-info	Contact Information.	string	Maximum length: 31	
engine-id	AC SNMP engineID string (maximum 24 characters).	string	Maximum length: 23	
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100	80
trap-high-mem-threshold	Memory usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100	80

config community

Parameter	Description	Type	Size	Default						
id	Community ID.	integer	Minimum value: 0 0 Maximum value: 4294967295							
name	Community name.	string	Maximum length: 35							
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
status	Enable/disable this SNMP community.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									

config hosts

Parameter	Description	Type	Size	Default
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

config user

Parameter	Description	Type	Size	Default
auth-proto	Authentication protocol.	option	-	sha
	Option	Description		
	md5	HMAC-MD5-96 authentication protocol.		
	sha	HMAC-SHA-96 authentication protocol.		
	sha224	HMAC-SHA224 authentication protocol.		
	sha256	HMAC-SHA256 authentication protocol.		
	sha384	HMAC-SHA384 authentication protocol.		
	sha512	HMAC-SHA512 authentication protocol.		
auth-pwd	Password for authentication protocol.	password	Not Specified	
name	SNMP user name.	string	Maximum length: 32	
notify-hosts	Configure SNMP User Notify Hosts.	ipv4-address	Not Specified	
priv-proto	Privacy (encryption) protocol.	option	-	aes
	Option	Description		
	aes	CFB128-AES-128 symmetric encryption protocol.		
	des	CBC-DES symmetric encryption protocol.		
	aes256	CFB128-AES-256 symmetric encryption protocol.		
	aes256cisco	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.		
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	

Parameter	Description	Type	Size	Default								
queries	Enable/disable SNMP queries for this user.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-auth-no-priv</i></td><td>Message with no authentication and no privacy (encryption).</td></tr><tr><td><i>auth-no-priv</i></td><td>Message with authentication but no privacy (encryption).</td></tr><tr><td><i>auth-priv</i></td><td>Message with authentication and privacy (encryption).</td></tr></table>	Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).			
Option	Description											
<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).											
<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).											
<i>auth-priv</i>	Message with authentication and privacy (encryption).											
status	SNMP user enable.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
trap-status	Enable/disable traps for this SNMP user.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

config wireless-controller ssid-policy

Configure WiFi SSID policies.

```

config wireless-controller ssid-policy
  Description: Configure WiFi SSID policies.
  edit <name>
    set description {var-string}
    set vlan {string}
  next
end

```

config wireless-controller ssid-policy

Parameter	Description	Type	Size	Default
description	Description.	var-string	Maximum length: 255	
name	Name.	string	Maximum length: 35	
vlan	VLAN interface name.	string	Maximum length: 35	

config wireless-controller syslog-profile

Configure Wireless Termination Points (WTP) system log server profile.

```
config wireless-controller syslog-profile
  Description: Configure Wireless Termination Points (WTP) system log server profile.
  edit <name>
    set comment {var-string}
    set log-level [emergency|alert|...]
    set server-addr-type [fqdn|ip]
    set server-fqdn {string}
    set server-ip {ipv4-address}
    set server-port {integer}
    set server-status [enable|disable]
    set server-type [standard|fortianalyzer]
  next
end
```

config wireless-controller syslog-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
log-level	Lowest level of log messages that FortiAP units send to this server (default = information).	option	-	information
	Option Description			
	<i>emergency</i>	Level 0		
	<i>alert</i>	Level 1		
	<i>critical</i>	Level 2		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error</i></td><td>Level 3</td></tr><tr><td><i>warning</i></td><td>Level 4</td></tr><tr><td><i>notification</i></td><td>Level 5</td></tr><tr><td><i>information</i></td><td>Level 6</td></tr><tr><td><i>debugging</i></td><td>Level 7</td></tr></table>	Option	Description	<i>error</i>	Level 3	<i>warning</i>	Level 4	<i>notification</i>	Level 5	<i>information</i>	Level 6	<i>debugging</i>	Level 7			
	Option	Description														
	<i>error</i>	Level 3														
	<i>warning</i>	Level 4														
	<i>notification</i>	Level 5														
	<i>information</i>	Level 6														
<i>debugging</i>	Level 7															
name	WTP system log server profile name.	string	Maximum length: 35													
server-addr-type	Syslog server address type (default = ip).	option	-	ip												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fqdn</i></td><td>Fully Qualified Domain Name address.</td></tr><tr><td><i>ip</i></td><td>IPv4 address.</td></tr></table>	Option	Description	<i>fqdn</i>	Fully Qualified Domain Name address.	<i>ip</i>	IPv4 address.									
	Option	Description														
	<i>fqdn</i>	Fully Qualified Domain Name address.														
<i>ip</i>	IPv4 address.															
server-fqdn	FQDN of syslog server that FortiAP units send log messages to.	string	Maximum length: 63													
server-ip	IP address of syslog server that FortiAP units send log messages to.	ipv4-address	Not Specified	0.0.0.0												
server-port	Port number of syslog server that FortiAP units send log messages to (default = 514).	integer	Minimum value: 0 Maximum value: 65535	514												
server-status	Enable/disable FortiAP units to send log messages to a syslog server (default = enable).	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable syslog server.</td></tr><tr><td><i>disable</i></td><td>Disable syslog server.</td></tr></table>	Option	Description	<i>enable</i>	Enable syslog server.	<i>disable</i>	Disable syslog server.									
	Option	Description														
	<i>enable</i>	Enable syslog server.														
<i>disable</i>	Disable syslog server.															
server-type	Configure syslog server type (default = standard).	option	-	standard												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard syslog server hosted on an server endpoint.</td></tr><tr><td><i>fortianalyzer</i></td><td>Syslog server hosted on a FortiAnalyzer device.</td></tr></table>	Option	Description	<i>standard</i>	Standard syslog server hosted on an server endpoint.	<i>fortianalyzer</i>	Syslog server hosted on a FortiAnalyzer device.									
	Option	Description														
	<i>standard</i>	Standard syslog server hosted on an server endpoint.														
<i>fortianalyzer</i>	Syslog server hosted on a FortiAnalyzer device.															

config wireless-controller timers

Configure CAPWAP timers.

```
config wireless-controller timers
  Description: Configure CAPWAP timers.
  set ap-reboot-wait-interval1 {integer}
  set ap-reboot-wait-interval2 {integer}
  set ap-reboot-wait-time {string}
  set auth-timeout {integer}
  set ble-device-cleanup {integer}
  set ble-scan-report-intv {integer}
  set client-idle-rehome-timeout {integer}
  set client-idle-timeout {integer}
  set discovery-interval {integer}
  set drma-interval {integer}
  set echo-interval {integer}
  set fake-ap-log {integer}
  set ipsec-intf-cleanup {integer}
  set nat-session-keep-alive {integer}
  set radio-stats-interval {integer}
  set rogue-ap-cleanup {integer}
  set rogue-ap-log {integer}
  set rogue-sta-cleanup {integer}
  set sta-cap-cleanup {integer}
  set sta-capability-interval {integer}
  set sta-locate-timer {integer}
  set sta-offline-cleanup {integer}
  set sta-offline-ip2mac-cleanup {integer}
  set sta-stats-interval {integer}
  set vap-stats-interval {integer}
  set wids-entry-cleanup {integer}
end
```

config wireless-controller timers

Parameter	Description	Type	Size	Default
ap-reboot-wait-interval1	Time in minutes to wait before AP reboots when there is no controller detected (5 - 65535, default = 0, 0 for no reboot).	integer	Minimum value: 5 Maximum value: 65535	0
ap-reboot-wait-interval2	Time in minutes to wait before AP reboots when there is no controller detected and standalone SSIDs are pushed to the AP in the previous session (5 - 65535, default = 0, 0 for no reboot).	integer	Minimum value: 5 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
ap-reboot-wait-time	Time to reboot the AP when there is no controller detected and standalone SSIDs are pushed to the AP in the previous session, format hh:mm.	string	Maximum length: 7	
auth-timeout	Time after which a client is considered failed in RADIUS authentication and times out (5 - 30 sec, default = 5).	integer	Minimum value: 5 Maximum value: 30	5
ble-device-cleanup	Time period in minutes to keep BLE device after it is gone (default = 60).	integer	Minimum value: 0 Maximum value: 4294967295	60
ble-scan-report-intv	Time between running Bluetooth Low Energy (BLE) reports (10 - 3600 sec, default = 30).	integer	Minimum value: 10 Maximum value: 3600	30
client-idle-rehome-timeout	Time after which a client is considered idle and disconnected from the home controller (2 - 3600 sec, default = 20, 0 for no timeout).	integer	Minimum value: 2 Maximum value: 3600	20
client-idle-timeout	Time after which a client is considered idle and times out (20 - 3600 sec, default = 300, 0 for no timeout).	integer	Minimum value: 20 Maximum value: 3600	300
discovery-interval	Time between discovery requests (2 - 180 sec, default = 5).	integer	Minimum value: 2 Maximum value: 180	5
drma-interval	Dynamic radio mode assignment (DRMA) schedule interval in minutes (1 - 1440, default = 60).	integer	Minimum value: 1 Maximum value: 1440	60
echo-interval	Time between echo requests sent by the managed WTP, AP, or FortiAP (1 - 255 sec, default = 30).	integer	Minimum value: 1 Maximum value: 255	30
fake-ap-log	Time between recording logs about fake APs if periodic fake AP logging is configured (1 - 1440 min, default = 1).	integer	Minimum value: 1 Maximum value: 1440	1
ipsec-intf-cleanup	Time period to keep IPsec VPN interfaces up after WTP sessions are disconnected (30 - 3600 sec, default = 120).	integer	Minimum value: 30 Maximum value: 3600	120
nat-session-keep-alive	Maximal time in seconds between control requests sent by the managed WTP, AP, or FortiAP (0 - 255 sec, default = 0).	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
radio-stats-interval	Time between running radio reports (1 - 255 sec, default = 15).	integer	Minimum value: 1 Maximum value: 255	15
rogue-ap-cleanup	Time period in minutes to keep rogue AP after it is gone (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
rogue-ap-log	Time between logging rogue AP messages if periodic rogue AP logging is configured (0 - 1440 min, default = 0).	integer	Minimum value: 0 Maximum value: 1440	0
rogue-sta-cleanup	Time period in minutes to keep rogue station after it is gone (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
sta-cap-cleanup	Time period in minutes to keep station capability data after it is gone (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0
sta-capability-interval	Time between running station capability reports (1 - 255 sec, default = 30).	integer	Minimum value: 1 Maximum value: 255	30
sta-locate-timer	Time between running client presence flushes to remove clients that are listed but no longer present (0 - 86400 sec, default = 1800).	integer	Minimum value: 0 Maximum value: 86400	1800
sta-offline-cleanup	Time period in seconds to keep station offline data after it is gone (default = 300).	integer	Minimum value: 0 Maximum value: 4294967295	300
sta-offline-ip2mac-cleanup	Time period in seconds to keep station offline ip2mac data after it is gone (default = 300).	integer	Minimum value: 0 Maximum value: 4294967295	300
sta-stats-interval	Time between running client (station) reports (1 - 255 sec, default = 10).	integer	Minimum value: 1 Maximum value: 255	10
vap-stats-interval	Time between running Virtual Access Point (VAP) reports (1 - 255 sec, default = 15).	integer	Minimum value: 1 Maximum value: 255	15
wids-entry-cleanup	Time period in minutes to keep wids entry after it is gone (default = 0).	integer	Minimum value: 0 Maximum value: 4294967295	0

config wireless-controller vap

Configure Virtual Access Points (VAPs).

```
config wireless-controller vap
  Description: Configure Virtual Access Points (VAPs).
  edit <name>
    set 80211k [disable|enable]
    set 80211v [disable|enable]
    set access-control-list {string}
    set additional-akms {option1}, {option2}, ...
    set address-group {string}
    set address-group-policy [disable|allow|...]
    set akm24-only [disable|enable]
    set antivirus-profile {string}
    set application-detection-engine [enable|disable]
    set application-dscp-marking [enable|disable]
    set application-list {string}
    set application-report-intv {integer}
    set atf-weight {integer}
    set auth [radius|usergroup]
    set auth-cert {string}
    set auth-portal-addr {string}
    set beacon-advertising {option1}, {option2}, ...
    set beacon-protection [disable|enable]
    set broadcast-ssid [enable|disable]
    set broadcast-suppression {option1}, {option2}, ...
    set bss-color-partial [enable|disable]
    set bstm-disassociation-imminent [enable|disable]
    set bstm-load-balancing-disassoc-timer {integer}
    set bstm-rssi-disassoc-timer {integer}
    set called-station-id-type [mac|ip|...]
    set captive-portal [enable|disable]
    set captive-portal-ac-name {string}
    set captive-portal-auth-timeout {integer}
    set captive-portal-fw-accounting [enable|disable]
    set dhcp-address-enforcement [enable|disable]
    set dhcp-lease-time {integer}
    set dhcp-option43-insertion [enable|disable]
    set dhcp-option82-circuit-id-insertion [style-1|style-2|...]
    set dhcp-option82-insertion [enable|disable]
    set dhcp-option82-remote-id-insertion [style-1|disable]
    set domain-name-stripping [disable|enable]
    set dynamic-vlan [enable|disable]
    set eap-reauth [enable|disable]
    set eap-reauth-intv {integer}
    set eapol-key-retries [disable|enable]
    set encrypt [TKIP|AES|...]
    set external-logout {string}
    set external-pre-auth [enable|disable]
    set external-web {var-string}
```



```

set external-web-format [auto-detect|no-query-string|...]
set fast-bss-transition [disable|enable]
set ft-mobility-domain {integer}
set ft-over-ds [disable|enable]
set ft-r0-key-lifetime {integer}
set gas-comeback-delay {integer}
set gas-fragmentation-limit {integer}
set gtk-rekey [enable|disable]
set gtk-rekey-intv {integer}
set high-efficiency [enable|disable]
set hotspot20-profile {string}
set igmp-snooping [enable|disable]
set intra-vap-privacy [enable|disable]
set ip {ipv4-classnet-host}
set ips-sensor {string}
set ipv6-rules {option1}, {option2}, ...
set key {password}
set keyindex {integer}
set l3-roaming [enable|disable]
set l3-roaming-mode [direct|indirect]
set ldpc [disable|rx|...]
set local-authentication [enable|disable]
set local-bridging [enable|disable]
set local-lan [allow|deny]
set local-lan-partition [enable|disable]
set local-standalone [enable|disable]
set local-standalone-dns [enable|disable]
set local-standalone-dns-ip {ipv4-address}
set local-standalone-nat [enable|disable]
set mac-auth-bypass [enable|disable]
set mac-called-station-delimiter [hyphen|single-hyphen|...]
set mac-calling-station-delimiter [hyphen|single-hyphen|...]
set mac-case [uppercase|lowercase]
set mac-password-delimiter [hyphen|single-hyphen|...]
set mac-username-delimiter [hyphen|single-hyphen|...]
set max-clients {integer}
set max-clients-ap {integer}
set mbo [disable|enable]
set mbo-cell-data-conn-pref [excluded|prefer-not|...]
set me-disable-thresh {integer}
set mesh-backhaul [enable|disable]
set mpsk-profile {string}
set mu-mimo [enable|disable]
set multicast-enhance [enable|disable]
set multicast-rate [0|6000|...]
set nac [enable|disable]
set nac-profile {string}
set nas-filter-rule [enable|disable]
set neighbor-report-dual-band [disable|enable]
set okc [disable|enable]
set osen [enable|disable]
set owe-groups {option1}, {option2}, ...

```

```

set owe-transition [disable|enable]
set owe-transition-ssid {string}
set passphrase {password}
set pmf [disable|enable|...]
set pmf-assoc-comeback-timeout {integer}
set pmf-sa-query-retry-timeout {integer}
set port-macauth [disable|radius|...]
set port-macauth-reauth-timeout {integer}
set port-macauth-timeout {integer}
set portal-message-override-group {string}
config portal-message-overrides
    Description: Individual message overrides.
    set auth-disclaimer-page {string}
    set auth-login-failed-page {string}
    set auth-login-page {string}
    set auth-reject-page {string}
end
set portal-type [auth|auth+disclaimer|...]
set pre-auth [enable|disable]
set primary-wag-profile {string}
set probe-resp-suppression [enable|disable]
set probe-resp-threshold {string}
set ptk-rekey [enable|disable]
set ptk-rekey-intv {integer}
set qos-profile {string}
set quarantine [enable|disable]
set radio-2g-threshold {string}
set radio-5g-threshold {string}
set radio-sensitivity [enable|disable]
set radius-mac-auth [enable|disable]
set radius-mac-auth-block-interval {integer}
set radius-mac-auth-server {string}
set radius-mac-auth-usergroups <name1>, <name2>, ...
set radius-mac-mpsk-auth [enable|disable]
set radius-mac-mpsk-timeout {integer}
set radius-server {string}
set rates-11a {option1}, {option2}, ...
set rates-11ac-mcs-map {string}
set rates-11ax-mcs-map {string}
set rates-11be-mcs-map {string}
set rates-11be-mcs-map-160 {string}
set rates-11be-mcs-map-320 {string}
set rates-11bg {option1}, {option2}, ...
set rates-11n-ss12 {option1}, {option2}, ...
set rates-11n-ss34 {option1}, {option2}, ...
set roaming-acct-interim-update [enable|disable]
set sae-groups {option1}, {option2}, ...
set sae-h2e-only [enable|disable]
set sae-hnp-only [enable|disable]
set sae-password {password}
set sae-pk [enable|disable]
set sae-private-key {string}

```

```

set scan-botnet-connections [disable|monitor|...]
set schedule <name1>, <name2>, ...
set secondary-wag-profile {string}
set security [open|wep64|...]
set security-exempt-list {string}
set security-redirect-url {var-string}
set selected-usergroups <name1>, <name2>, ...
set split-tunneling [enable|disable]
set ssid {string}
set sticky-client-remove [enable|disable]
set sticky-client-threshold-2g {string}
set sticky-client-threshold-5g {string}
set sticky-client-threshold-6g {string}
set target-wake-time [enable|disable]
set tkip-counter-measure [enable|disable]
set tunnel-echo-interval {integer}
set tunnel-fallback-interval {integer}
set usergroup <name1>, <name2>, ...
set utm-log [enable|disable]
set utm-profile {string}
set utm-status [enable|disable]
set vlan-auto [enable|disable]
config vlan-name
    Description: Table for mapping VLAN name to VLAN ID.
    edit <name>
        set vlan-id {integer}
    next
end
config vlan-pool
    Description: VLAN pool.
    edit <id>
        set wtp-group {string}
    next
end
set vlan-pooling [wtp-group|round-robin|...]
set vlanid {integer}
set webfilter-profile {string}
next
end

```

config wireless-controller vap

Parameter	Description	Type	Size	Default
80211k	Enable/disable 802.11k assisted roaming (default = enable).	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable 802.11k assisted roaming.		
	<i>enable</i>	Enable 802.11k assisted roaming.		
80211v	Enable/disable 802.11v assisted roaming (default = enable).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable 802.11v assisted roaming.		
	<i>enable</i>	Enable 802.11v assisted roaming.		
access-control-list	Profile name for access-control-list.	string	Maximum length: 35	
additional-akms	Additional AKMs.	option	-	
	Option	Description		
	<i>akm6</i>	Use AKM suite employing PSK_SHA256.		
	<i>akm24</i>	Use AKM suite employing SAE_EXT.		
address-group	Firewall Address Group Name.	string	Maximum length: 79	
address-group-policy	Configure MAC address filtering policy for MAC addresses that are in the address-group.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable MAC address filtering policy for MAC addresses that are in the address-group		
	<i>allow</i>	Allow clients with MAC addresses that are in the address-group.		
	<i>deny</i>	Block clients with MAC addresses that are in the address-group.		
akm24-only	WPA3 SAE using group-dependent hash only (default = disable).	option	-	disable
	Option	Description		
	<i>disable</i>	Disable WPA3 SAE using group-dependent hash only.		
	<i>enable</i>	Enable WPA3 SAE using group-dependent hash only.		
antivirus-profile	AntiVirus profile name.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default								
application-detection-engine	Enable/disable application detection engine (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable application detection engine.</td></tr><tr><td><i>disable</i></td><td>Disable application detection engine.</td></tr></table>	Option	Description	<i>enable</i>	Enable application detection engine.	<i>disable</i>	Disable application detection engine.					
Option	Description											
<i>enable</i>	Enable application detection engine.											
<i>disable</i>	Disable application detection engine.											
application-dscp-marking	Enable/disable application attribute based DSCP marking (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable application based DSCP marking.</td></tr><tr><td><i>disable</i></td><td>Disable application based DSCP marking.</td></tr></table>	Option	Description	<i>enable</i>	Enable application based DSCP marking.	<i>disable</i>	Disable application based DSCP marking.					
Option	Description											
<i>enable</i>	Enable application based DSCP marking.											
<i>disable</i>	Disable application based DSCP marking.											
application-list	Application control list name.	string	Maximum length: 47									
application-report-intv	Application report interval (30 - 864000 sec, default = 120).	integer	Minimum value: 30 Maximum value: 864000	120								
atf-weight	Airtime weight in percentage (default = 20).	integer	Minimum value: 0 Maximum value: 100	20								
auth	Authentication protocol.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>radius</i></td><td>Use a RADIUS server to authenticate clients.</td></tr><tr><td><i>usergroup</i></td><td>Use a firewall usergroup to authenticate clients.</td></tr></table>	Option	Description	<i>radius</i>	Use a RADIUS server to authenticate clients.	<i>usergroup</i>	Use a firewall usergroup to authenticate clients.					
Option	Description											
<i>radius</i>	Use a RADIUS server to authenticate clients.											
<i>usergroup</i>	Use a firewall usergroup to authenticate clients.											
auth-cert	HTTPS server certificate.	string	Maximum length: 35									
auth-portal-addr	Address of captive portal.	string	Maximum length: 63									
beacon-advertising	Fortinet beacon advertising IE data (default = empty).	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>name</i></td><td>AP name.</td></tr><tr><td><i>model</i></td><td>AP model abbreviation.</td></tr><tr><td><i>serial-number</i></td><td>AP serial number.</td></tr></table>	Option	Description	<i>name</i>	AP name.	<i>model</i>	AP model abbreviation.	<i>serial-number</i>	AP serial number.			
Option	Description											
<i>name</i>	AP name.											
<i>model</i>	AP model abbreviation.											
<i>serial-number</i>	AP serial number.											

Parameter	Description	Type	Size	Default																														
beacon-protection	Enable/disable beacon protection support (default = disable).	option	-	disable																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable beacon protection.</td></tr><tr><td><i>enable</i></td><td>Enable beacon protection.</td></tr></table>	Option	Description	<i>disable</i>	Disable beacon protection.	<i>enable</i>	Enable beacon protection.																											
Option	Description																																	
<i>disable</i>	Disable beacon protection.																																	
<i>enable</i>	Enable beacon protection.																																	
broadcast-ssid	Enable/disable broadcasting the SSID (default = enable).	option	-	enable																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcasting the SSID.</td></tr><tr><td><i>disable</i></td><td>Disable broadcasting the SSID.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcasting the SSID.	<i>disable</i>	Disable broadcasting the SSID.																											
Option	Description																																	
<i>enable</i>	Enable broadcasting the SSID.																																	
<i>disable</i>	Disable broadcasting the SSID.																																	
broadcast-suppression	Optional suppression of broadcast messages. For example, you can keep DHCP messages, ARP broadcasts, and so on off of the wireless network.	option	-	dhcp-up dhcp-ucast arp-known																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dhcp-up</i></td><td>Suppress broadcast uplink DHCP messages.</td></tr><tr><td><i>dhcp-down</i></td><td>Suppress broadcast downlink DHCP messages.</td></tr><tr><td><i>dhcp-starvation</i></td><td>Suppress broadcast DHCP starvation req messages.</td></tr><tr><td><i>dhcp-ucast</i></td><td>Convert downlink broadcast DHCP messages to unicast messages.</td></tr><tr><td><i>arp-known</i></td><td>Suppress broadcast ARP for known wireless clients.</td></tr><tr><td><i>arp-unknown</i></td><td>Suppress broadcast ARP for unknown wireless clients.</td></tr><tr><td><i>arp-reply</i></td><td>Suppress broadcast ARP reply from wireless clients.</td></tr><tr><td><i>arp-poison</i></td><td>Suppress ARP poison messages from wireless clients.</td></tr><tr><td><i>arp-proxy</i></td><td>Reply ARP requests for wireless clients as a proxy.</td></tr><tr><td><i>netbios-ns</i></td><td>Suppress NetBIOS name services packets with UDP port 137.</td></tr><tr><td><i>netbios-ds</i></td><td>Suppress NetBIOS datagram services packets with UDP port 138.</td></tr><tr><td><i>ipv6</i></td><td>Suppress IPv6 packets.</td></tr><tr><td><i>all-other-mc</i></td><td>Suppress all other multicast messages.</td></tr><tr><td><i>all-other-bc</i></td><td>Suppress all other broadcast messages.</td></tr></table>	Option	Description	<i>dhcp-up</i>	Suppress broadcast uplink DHCP messages.	<i>dhcp-down</i>	Suppress broadcast downlink DHCP messages.	<i>dhcp-starvation</i>	Suppress broadcast DHCP starvation req messages.	<i>dhcp-ucast</i>	Convert downlink broadcast DHCP messages to unicast messages.	<i>arp-known</i>	Suppress broadcast ARP for known wireless clients.	<i>arp-unknown</i>	Suppress broadcast ARP for unknown wireless clients.	<i>arp-reply</i>	Suppress broadcast ARP reply from wireless clients.	<i>arp-poison</i>	Suppress ARP poison messages from wireless clients.	<i>arp-proxy</i>	Reply ARP requests for wireless clients as a proxy.	<i>netbios-ns</i>	Suppress NetBIOS name services packets with UDP port 137.	<i>netbios-ds</i>	Suppress NetBIOS datagram services packets with UDP port 138.	<i>ipv6</i>	Suppress IPv6 packets.	<i>all-other-mc</i>	Suppress all other multicast messages.	<i>all-other-bc</i>	Suppress all other broadcast messages.			
Option	Description																																	
<i>dhcp-up</i>	Suppress broadcast uplink DHCP messages.																																	
<i>dhcp-down</i>	Suppress broadcast downlink DHCP messages.																																	
<i>dhcp-starvation</i>	Suppress broadcast DHCP starvation req messages.																																	
<i>dhcp-ucast</i>	Convert downlink broadcast DHCP messages to unicast messages.																																	
<i>arp-known</i>	Suppress broadcast ARP for known wireless clients.																																	
<i>arp-unknown</i>	Suppress broadcast ARP for unknown wireless clients.																																	
<i>arp-reply</i>	Suppress broadcast ARP reply from wireless clients.																																	
<i>arp-poison</i>	Suppress ARP poison messages from wireless clients.																																	
<i>arp-proxy</i>	Reply ARP requests for wireless clients as a proxy.																																	
<i>netbios-ns</i>	Suppress NetBIOS name services packets with UDP port 137.																																	
<i>netbios-ds</i>	Suppress NetBIOS datagram services packets with UDP port 138.																																	
<i>ipv6</i>	Suppress IPv6 packets.																																	
<i>all-other-mc</i>	Suppress all other multicast messages.																																	
<i>all-other-bc</i>	Suppress all other broadcast messages.																																	

Parameter	Description	Type	Size	Default								
bss-color-partial	Enable/disable 802.11ax partial BSS color (default = enable).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11ax partial BSS color.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11ax partial BSS color.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11ax partial BSS color.	<i>disable</i>	Disable 802.11ax partial BSS color.					
Option	Description											
<i>enable</i>	Enable 802.11ax partial BSS color.											
<i>disable</i>	Disable 802.11ax partial BSS color.											
bstm-disassociation-imminent	Enable/disable forcing of disassociation after the BSTM request timer has been reached (default = enable).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable BSTM disassociation imminent.</td></tr><tr><td><i>disable</i></td><td>Disable BSTM disassociation imminent.</td></tr></table>	Option	Description	<i>enable</i>	Enable BSTM disassociation imminent.	<i>disable</i>	Disable BSTM disassociation imminent.					
Option	Description											
<i>enable</i>	Enable BSTM disassociation imminent.											
<i>disable</i>	Disable BSTM disassociation imminent.											
bstm-load-balancing-disassoc-timer	Time interval for client to voluntarily leave AP before forcing a disassociation due to AP load-balancing (0 to 30, default = 10).	integer	Minimum value: 10 Maximum value: 30									
bstm-rssi-disassoc-timer	Time interval for client to voluntarily leave AP before forcing a disassociation due to low RSSI (0 to 2000, default = 200).	integer	Minimum value: 200 Maximum value: 2000									
called-station-id-type	The format type of RADIUS attribute Called-Station-Id (default = mac).	option	-	mac								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mac</i></td><td>Use MAC:SSID format.</td></tr><tr><td><i>ip</i></td><td>Use IP:SSID format.</td></tr><tr><td><i>apname</i></td><td>Use APName:SSID format.</td></tr></table>	Option	Description	<i>mac</i>	Use MAC:SSID format.	<i>ip</i>	Use IP:SSID format.	<i>apname</i>	Use APName:SSID format.			
Option	Description											
<i>mac</i>	Use MAC:SSID format.											
<i>ip</i>	Use IP:SSID format.											
<i>apname</i>	Use APName:SSID format.											
captive-portal	Enable/disable captive portal.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable captive portal.</td></tr><tr><td><i>disable</i></td><td>Disable captive portal.</td></tr></table>	Option	Description	<i>enable</i>	Enable captive portal.	<i>disable</i>	Disable captive portal.					
Option	Description											
<i>enable</i>	Enable captive portal.											
<i>disable</i>	Disable captive portal.											
captive-portal-ac-name	Local-bridging captive portal ac-name.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
captive-portal-auth-timeout	Hard timeout - AP will always clear the session after timeout regardless of traffic (0 - 864000 sec, default = 0).	integer	Minimum value: 0 Maximum value: 864000	0						
captive-portal-fw-accounting	Enable/disable RADIUS accounting for captive portal firewall authentication session.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable RADIUS accounting for captive portal firewall authentication session.</td></tr><tr><td>disable</td><td>Disable RADIUS accounting for captive portal firewall authentication session.</td></tr></table>	Option	Description	enable	Enable RADIUS accounting for captive portal firewall authentication session.	disable	Disable RADIUS accounting for captive portal firewall authentication session.			
Option	Description									
enable	Enable RADIUS accounting for captive portal firewall authentication session.									
disable	Disable RADIUS accounting for captive portal firewall authentication session.									
dhcp-address-enforcement	Enable/disable DHCP address enforcement (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DHCP enforcement, data from clients that have not completed the DHCP process will be blocked.</td></tr><tr><td>disable</td><td>Disable DHCP enforcement, clients can access the network without DHCP process.</td></tr></table>	Option	Description	enable	Enable DHCP enforcement, data from clients that have not completed the DHCP process will be blocked.	disable	Disable DHCP enforcement, clients can access the network without DHCP process.			
Option	Description									
enable	Enable DHCP enforcement, data from clients that have not completed the DHCP process will be blocked.									
disable	Disable DHCP enforcement, clients can access the network without DHCP process.									
dhcp-lease-time	DHCP lease time in seconds for NAT IP address.	integer	Minimum value: 300 Maximum value: 8640000	2400						
dhcp-option43-insertion	Enable/disable insertion of DHCP option 43 (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable insertion of DHCP option 43.</td></tr><tr><td>disable</td><td>Disable insertion of DHCP option 43.</td></tr></table>	Option	Description	enable	Enable insertion of DHCP option 43.	disable	Disable insertion of DHCP option 43.			
Option	Description									
enable	Enable insertion of DHCP option 43.									
disable	Disable insertion of DHCP option 43.									
dhcp-option82-circuit-id-insertion	Enable/disable DHCP option 82 circuit-id insert (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>style-1</td><td>ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".</td></tr><tr><td>style-2</td><td>ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".</td></tr></table>	Option	Description	style-1	ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".	style-2	ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".			
Option	Description									
style-1	ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".									
style-2	ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>style-3</td><td>ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example, "WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".</td></tr><tr><td>disable</td><td>Disable DHCP option 82 circuit-id insert.</td></tr></table>	Option	Description	style-3	ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example, "WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".	disable	Disable DHCP option 82 circuit-id insert.			
	Option	Description								
	style-3	ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example, "WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".								
disable	Disable DHCP option 82 circuit-id insert.									
dhcp-option82-insertion	Enable/disable DHCP option 82 insert (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DHCP option 82 insert.</td></tr><tr><td>disable</td><td>Disable DHCP option 82 insert.</td></tr></table>	Option	Description	enable	Enable DHCP option 82 insert.	disable	Disable DHCP option 82 insert.			
	Option	Description								
	enable	Enable DHCP option 82 insert.								
disable	Disable DHCP option 82 insert.									
dhcp-option82-remote-id-insertion	Enable/disable DHCP option 82 remote-id insert (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>style-1</td><td>ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.</td></tr><tr><td>disable</td><td>Disable DHCP option 82 remote-id insert.</td></tr></table>	Option	Description	style-1	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.	disable	Disable DHCP option 82 remote-id insert.			
	Option	Description								
	style-1	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.								
disable	Disable DHCP option 82 remote-id insert.									
domain-name-stripping	Enable/disable stripping domain name from identity (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable stripping domain name from identity.</td></tr><tr><td>enable</td><td>Enable stripping domain name from identity.</td></tr></table>	Option	Description	disable	Disable stripping domain name from identity.	enable	Enable stripping domain name from identity.			
	Option	Description								
	disable	Disable stripping domain name from identity.								
enable	Enable stripping domain name from identity.									
dynamic-vlan	Enable/disable dynamic VLAN assignment.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dynamic VLAN assignment.</td></tr><tr><td>disable</td><td>Disable dynamic VLAN assignment.</td></tr></table>	Option	Description	enable	Enable dynamic VLAN assignment.	disable	Disable dynamic VLAN assignment.			
	Option	Description								
	enable	Enable dynamic VLAN assignment.								
disable	Disable dynamic VLAN assignment.									
eap-reauth	Enable/disable EAP re-authentication for WPA-Enterprise security.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAP re-authentication for WPA-Enterprise security.</td></tr><tr><td><i>disable</i></td><td>Disable EAP re-authentication for WPA-Enterprise security.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAP re-authentication for WPA-Enterprise security.	<i>disable</i>	Disable EAP re-authentication for WPA-Enterprise security.					
	Option	Description										
	<i>enable</i>	Enable EAP re-authentication for WPA-Enterprise security.										
<i>disable</i>	Disable EAP re-authentication for WPA-Enterprise security.											
eap-reauth-intv	EAP re-authentication interval (1800 - 864000 sec, default = 86400).	integer	Minimum value: 1800 Maximum value: 864000	86400								
eapol-key-retries	Enable/disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2) (default = enable).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).</td></tr><tr><td><i>enable</i></td><td>Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).</td></tr></table>	Option	Description	<i>disable</i>	Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).	<i>enable</i>	Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).					
	Option	Description										
	<i>disable</i>	Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).										
<i>enable</i>	Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).											
encrypt	Encryption protocol to use (only available when security is set to a WPA type).	option	-	AES								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TKIP</i></td><td>Use TKIP encryption.</td></tr><tr><td><i>AES</i></td><td>Use AES encryption.</td></tr><tr><td><i>TKIP-AES</i></td><td>Use TKIP and AES encryption.</td></tr></table>	Option	Description	<i>TKIP</i>	Use TKIP encryption.	<i>AES</i>	Use AES encryption.	<i>TKIP-AES</i>	Use TKIP and AES encryption.			
	Option	Description										
	<i>TKIP</i>	Use TKIP encryption.										
	<i>AES</i>	Use AES encryption.										
<i>TKIP-AES</i>	Use TKIP and AES encryption.											
external-logout	URL of external authentication logout server.	string	Maximum length: 127									
external-pre-auth	Enable/disable pre-authentication with external APs not managed by the FortiGate (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pre-authentication with external APs.</td></tr><tr><td><i>disable</i></td><td>Disable pre-authentication with external APs.</td></tr></table>	Option	Description	<i>enable</i>	Enable pre-authentication with external APs.	<i>disable</i>	Disable pre-authentication with external APs.					
	Option	Description										
	<i>enable</i>	Enable pre-authentication with external APs.										
<i>disable</i>	Disable pre-authentication with external APs.											
external-web	URL of external authentication web server.	var-string	Maximum length: 1023									
external-web-format	URL query parameter detection (default = auto-detect).	option	-	auto-detect								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto-detect</i>	Automatically detect if "external-web" URL has any query parameter.		
	<i>no-query-string</i>	"external-web" URL does not have any query parameter.		
	<i>partial-query-string</i>	"external-web" URL has some query parameters.		
fast-bss-transition	Enable/disable 802.11r Fast BSS Transition (FT) (default = disable).	option	-	disable
	Option	Description		
	<i>disable</i>	Disable 802.11r Fast BSS Transition (FT).		
	<i>enable</i>	Enable 802.11r Fast BSS Transition (FT).		
ft-mobility-domain	Mobility domain identifier in FT (1 - 65535, default = 1000).	integer	Minimum value: 1 Maximum value: 65535	1000
ft-over-ds	Enable/disable FT over the Distribution System (DS).	option	-	disable
	Option	Description		
	<i>disable</i>	Disable FT over the Distribution System (DS).		
	<i>enable</i>	Enable FT over the Distribution System (DS).		
ft-r0-key-lifetime	Lifetime of the PMK-R0 key in FT, 1-65535 minutes.	integer	Minimum value: 1 Maximum value: 65535	480
gas-comeback-delay	GAS comeback delay (0 or 100 - 10000 milliseconds, default = 500).	integer	Minimum value: 100 Maximum value: 10000	500
gas-fragmentation-limit	GAS fragmentation limit (512 - 4096, default = 1024).	integer	Minimum value: 512 Maximum value: 4096	1024
gtk-rekey	Enable/disable GTK rekey for WPA security.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable GTK rekey for WPA security.		
	<i>disable</i>	Disable GTK rekey for WPA security.		

Parameter	Description	Type	Size	Default
gtk-rekey-intv	GTK rekey interval (600 - 864000 sec, default = 86400).	integer	Minimum value: 600 Maximum value: 864000	86400
high-efficiency	Enable/disable 802.11ax high efficiency (default = enable).	option	-	enable
	Option	Description		
	enable	Enable 802.11ax high efficiency.		
	disable	Disable 802.11ax high efficiency.		
hotspot20-profile	Hotspot 2.0 profile name.	string	Maximum length: 35	
igmp-snooping	Enable/disable IGMP snooping.	option	-	disable
	Option	Description		
	enable	Enable IGMP snooping.		
	disable	Disable IGMP snooping.		
intra-vap-privacy	Enable/disable blocking communication between clients on the same SSID (called intra-SSID privacy) (default = disable).	option	-	disable
	Option	Description		
	enable	Enable intra-SSID privacy.		
	disable	Disable intra-SSID privacy.		
ip	IP address and subnet mask for the local standalone NAT subnet.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
ips-sensor	IPS sensor name.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default																				
ipv6-rules	Optional rules of IPv6 packets. For example, you can keep RA, RS and so on off of the wireless network.	option	-	drop-icmp6ra drop-icmp6rs drop-llmnr6 drop-icmp6mld2 drop-dhcp6s drop-dhcp6c ndp-proxy drop-ns-dad																				
<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop-icmp6ra</td><td>Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.</td></tr><tr><td>drop-icmp6rs</td><td>Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.</td></tr><tr><td>drop-llmnr6</td><td>Drop Link-Local Multicast Name Resolution (LLMNR) packets</td></tr><tr><td>drop-icmp6mld2</td><td>Drop ICMP6 Multicast Listener Report V2 (MLD2) packets</td></tr><tr><td>drop-dhcp6s</td><td>Drop DHCP6 server generated packets that originate from wireless clients.</td></tr><tr><td>drop-dhcp6c</td><td>Drop DHCP6 client generated packets to be sent to wireless clients.</td></tr><tr><td>ndp-proxy</td><td>Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.</td></tr><tr><td>drop-ns-dad</td><td>Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.</td></tr><tr><td>drop-ns-nondad</td><td>Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.</td></tr></table>					Option	Description	drop-icmp6ra	Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.	drop-icmp6rs	Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.	drop-llmnr6	Drop Link-Local Multicast Name Resolution (LLMNR) packets	drop-icmp6mld2	Drop ICMP6 Multicast Listener Report V2 (MLD2) packets	drop-dhcp6s	Drop DHCP6 server generated packets that originate from wireless clients.	drop-dhcp6c	Drop DHCP6 client generated packets to be sent to wireless clients.	ndp-proxy	Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.	drop-ns-dad	Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.	drop-ns-nondad	Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.
Option	Description																							
drop-icmp6ra	Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.																							
drop-icmp6rs	Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.																							
drop-llmnr6	Drop Link-Local Multicast Name Resolution (LLMNR) packets																							
drop-icmp6mld2	Drop ICMP6 Multicast Listener Report V2 (MLD2) packets																							
drop-dhcp6s	Drop DHCP6 server generated packets that originate from wireless clients.																							
drop-dhcp6c	Drop DHCP6 client generated packets to be sent to wireless clients.																							
ndp-proxy	Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.																							
drop-ns-dad	Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.																							
drop-ns-nondad	Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.																							
key	WEP Key.	password	Not Specified																					
keyindex	WEP key index (1 - 4).	integer	Minimum value: 1 1 Maximum value: 4																					
l3-roaming	Enable/disable layer 3 roaming (default = disable).	option	-	disable																				
<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable layer 3 roaming.</td></tr><tr><td>disable</td><td>Disable layer 3 roaming.</td></tr></table>					Option	Description	enable	Enable layer 3 roaming.	disable	Disable layer 3 roaming.														
Option	Description																							
enable	Enable layer 3 roaming.																							
disable	Disable layer 3 roaming.																							

Parameter	Description	Type	Size	Default										
l3-roaming-mode	Select the way that layer 3 roaming traffic is passed (default = direct).	option	-	direct										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>direct</td><td>Layer 3 roaming traffic is passed between home AP and guest AP directly.</td></tr><tr><td>indirect</td><td>Layer 3 roaming traffic is passed between home AP and guest AP through controllers.</td></tr></table>	Option	Description	direct	Layer 3 roaming traffic is passed between home AP and guest AP directly.	indirect	Layer 3 roaming traffic is passed between home AP and guest AP through controllers.							
Option	Description													
direct	Layer 3 roaming traffic is passed between home AP and guest AP directly.													
indirect	Layer 3 roaming traffic is passed between home AP and guest AP through controllers.													
ldpc	VAP low-density parity-check (LDPC) coding configuration.	option	-	rxtx										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable LDPC.</td></tr><tr><td>rx</td><td>Enable LDPC when receiving traffic.</td></tr><tr><td>tx</td><td>Enable LDPC when transmitting traffic.</td></tr><tr><td>rxtx</td><td>Enable LDPC when both receiving and transmitting traffic.</td></tr></table>	Option	Description	disable	Disable LDPC.	rx	Enable LDPC when receiving traffic.	tx	Enable LDPC when transmitting traffic.	rxtx	Enable LDPC when both receiving and transmitting traffic.			
Option	Description													
disable	Disable LDPC.													
rx	Enable LDPC when receiving traffic.													
tx	Enable LDPC when transmitting traffic.													
rxtx	Enable LDPC when both receiving and transmitting traffic.													
local-authentication	Enable/disable AP local authentication.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable AP local authentication.</td></tr><tr><td>disable</td><td>Disable AP local authentication.</td></tr></table>	Option	Description	enable	Enable AP local authentication.	disable	Disable AP local authentication.							
Option	Description													
enable	Enable AP local authentication.													
disable	Disable AP local authentication.													
local-bridging	Enable/disable bridging of wireless and Ethernet interfaces on the FortiAP (default = disable).	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable AP local VAP to Ethernet bridging.</td></tr><tr><td>disable</td><td>Disable AP local VAP to Ethernet bridging.</td></tr></table>	Option	Description	enable	Enable AP local VAP to Ethernet bridging.	disable	Disable AP local VAP to Ethernet bridging.							
Option	Description													
enable	Enable AP local VAP to Ethernet bridging.													
disable	Disable AP local VAP to Ethernet bridging.													
local-lan	Allow/deny traffic destined for a Class A, B, or C private IP address (default = allow).	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow traffic destined for a Class A, B, or C private IP address.</td></tr><tr><td>deny</td><td>Deny traffic destined for a Class A, B, or C private IP address.</td></tr></table>	Option	Description	allow	Allow traffic destined for a Class A, B, or C private IP address.	deny	Deny traffic destined for a Class A, B, or C private IP address.							
Option	Description													
allow	Allow traffic destined for a Class A, B, or C private IP address.													
deny	Deny traffic destined for a Class A, B, or C private IP address.													

Parameter	Description	Type	Size	Default						
local-lan-partition	Enable/disable segregating client traffic to local LAN side (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable AP local LAN segregation.</td></tr><tr><td>disable</td><td>Disable AP local LAN segregation.</td></tr></table>	Option	Description	enable	Enable AP local LAN segregation.	disable	Disable AP local LAN segregation.			
Option	Description									
enable	Enable AP local LAN segregation.									
disable	Disable AP local LAN segregation.									
local-standalone	Enable/disable AP local standalone (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable AP local standalone.</td></tr><tr><td>disable</td><td>Disable AP local standalone.</td></tr></table>	Option	Description	enable	Enable AP local standalone.	disable	Disable AP local standalone.			
Option	Description									
enable	Enable AP local standalone.									
disable	Disable AP local standalone.									
local-standalone-dns	Enable/disable AP local standalone DNS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable AP local standalone DNS.</td></tr><tr><td>disable</td><td>Disable AP local standalone DNS.</td></tr></table>	Option	Description	enable	Enable AP local standalone DNS.	disable	Disable AP local standalone DNS.			
Option	Description									
enable	Enable AP local standalone DNS.									
disable	Disable AP local standalone DNS.									
local-standalone-dns-ip	IPv4 addresses for the local standalone DNS.	ipv4-address	Not Specified							
local-standalone-nat	Enable/disable AP local standalone NAT mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable AP local standalone NAT mode.</td></tr><tr><td>disable</td><td>Disable AP local standalone NAT mode.</td></tr></table>	Option	Description	enable	Enable AP local standalone NAT mode.	disable	Disable AP local standalone NAT mode.			
Option	Description									
enable	Enable AP local standalone NAT mode.									
disable	Disable AP local standalone NAT mode.									
mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable MAC authentication bypass.</td></tr><tr><td>disable</td><td>Disable MAC authentication bypass.</td></tr></table>	Option	Description	enable	Enable MAC authentication bypass.	disable	Disable MAC authentication bypass.			
Option	Description									
enable	Enable MAC authentication bypass.									
disable	Disable MAC authentication bypass.									
mac-called-station-delimiter	MAC called station delimiter (default = hyphen).	option	-	hyphen						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>hyphen</i>	Use hyphen as delimiter for called station.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for called station.		
	<i>colon</i>	Use colon as delimiter for called station.		
	<i>none</i>	No delimiter for called station.		
mac-calling-station-delimiter	MAC calling station delimiter (default = hyphen).	option	-	hyphen
	Option Description			
	<i>hyphen</i>	Use hyphen as delimiter for calling station.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for calling station.		
	<i>colon</i>	Use colon as delimiter for calling station.		
	<i>none</i>	No delimiter for calling station.		
mac-case	MAC case (default = uppercase).	option	-	uppercase
	Option Description			
	<i>uppercase</i>	Use uppercase MAC.		
	<i>lowercase</i>	Use lowercase MAC.		
mac-password-delimiter	MAC authentication password delimiter (default = hyphen).	option	-	hyphen
	Option Description			
	<i>hyphen</i>	Use hyphen as delimiter for MAC auth password.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC auth password.		
	<i>colon</i>	Use colon as delimiter for MAC auth password.		
	<i>none</i>	No delimiter for MAC auth password.		
mac-username-delimiter	MAC authentication username delimiter (default = hyphen).	option	-	hyphen
	Option Description			
	<i>hyphen</i>	Use hyphen as delimiter for MAC auth username.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC auth username.		
	<i>colon</i>	Use colon as delimiter for MAC auth username.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No delimiter for MAC auth username.</td></tr></table>	Option	Description	<i>none</i>	No delimiter for MAC auth username.							
Option	Description											
<i>none</i>	No delimiter for MAC auth username.											
max-clients	Maximum number of clients that can connect simultaneously to the VAP (default = 0, meaning no limitation).	integer	Minimum value: 0 Maximum value: 4294967295	0								
max-clients-ap	Maximum number of clients that can connect simultaneously to the VAP per AP radio (default = 0, meaning no limitation).	integer	Minimum value: 0 Maximum value: 4294967295	0								
mbo	Enable/disable Multiband Operation (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Multiband Operation (MBO).</td></tr><tr><td><i>enable</i></td><td>Enable Multiband Operation (MBO).</td></tr></table>	Option	Description	<i>disable</i>	Disable Multiband Operation (MBO).	<i>enable</i>	Enable Multiband Operation (MBO).					
Option	Description											
<i>disable</i>	Disable Multiband Operation (MBO).											
<i>enable</i>	Enable Multiband Operation (MBO).											
mbo-cell-data-conn-pref	MBO cell data connection preference (0, 1, or 255, default = 1).	option	-	prefer-not								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>excluded</i></td><td>Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection.</td></tr><tr><td><i>prefer-not</i></td><td>Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should not use cellular data connection.</td></tr><tr><td><i>prefer-use</i></td><td>Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should use cellular data connection.</td></tr></table>	Option	Description	<i>excluded</i>	Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection.	<i>prefer-not</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should not use cellular data connection.	<i>prefer-use</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should use cellular data connection.			
Option	Description											
<i>excluded</i>	Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection.											
<i>prefer-not</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should not use cellular data connection.											
<i>prefer-use</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should use cellular data connection.											
me-disable-thresh	Disable multicast enhancement when this many clients are receiving multicast traffic.	integer	Minimum value: 32 Maximum value: 256	32								
mesh-backhaul	Enable/disable using this VAP as a WiFi mesh backhaul (default = disable). This entry is only available when security is set to a WPA type or open.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable mesh backhaul.</td></tr><tr><td><i>disable</i></td><td>Disable mesh backhaul.</td></tr></table>	Option	Description	<i>enable</i>	Enable mesh backhaul.	<i>disable</i>	Disable mesh backhaul.					
Option	Description											
<i>enable</i>	Enable mesh backhaul.											
<i>disable</i>	Disable mesh backhaul.											

Parameter	Description	Type	Size	Default										
mpsk-profile	MPSK profile name.	string	Maximum length: 35											
mu-mimo	Enable/disable Multi-user MIMO (default = enable).	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Multi-user MIMO.</td></tr><tr><td><i>disable</i></td><td>Disable Multi-user MIMO.</td></tr></table>	Option	Description	<i>enable</i>	Enable Multi-user MIMO.	<i>disable</i>	Disable Multi-user MIMO.							
Option	Description													
<i>enable</i>	Enable Multi-user MIMO.													
<i>disable</i>	Disable Multi-user MIMO.													
multicast-enhance	Enable/disable converting multicast to unicast to improve performance (default = disable).	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast enhancement.</td></tr><tr><td><i>disable</i></td><td>Disable multicast enhancement.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast enhancement.	<i>disable</i>	Disable multicast enhancement.							
Option	Description													
<i>enable</i>	Enable multicast enhancement.													
<i>disable</i>	Disable multicast enhancement.													
multicast-rate	Multicast rate (0, 6000, 12000, or 24000 kbps, default = 0).	option	-	0										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>0</i></td><td>Use the default multicast rate.</td></tr><tr><td><i>6000</i></td><td>6 Mbps.</td></tr><tr><td><i>12000</i></td><td>12 Mbps.</td></tr><tr><td><i>24000</i></td><td>24 Mbps.</td></tr></table>	Option	Description	<i>0</i>	Use the default multicast rate.	<i>6000</i>	6 Mbps.	<i>12000</i>	12 Mbps.	<i>24000</i>	24 Mbps.			
Option	Description													
<i>0</i>	Use the default multicast rate.													
<i>6000</i>	6 Mbps.													
<i>12000</i>	12 Mbps.													
<i>24000</i>	24 Mbps.													
nac	Enable/disable network access control.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable network access control.</td></tr><tr><td><i>disable</i></td><td>Disable network access control.</td></tr></table>	Option	Description	<i>enable</i>	Enable network access control.	<i>disable</i>	Disable network access control.							
Option	Description													
<i>enable</i>	Enable network access control.													
<i>disable</i>	Disable network access control.													
nac-profile	NAC profile name.	string	Maximum length: 35											
name	Virtual AP name.	string	Maximum length: 15											
nas-filter-rule	Enable/disable NAS filter rule support (default = disable).	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable NAS filter rule for RADIUS server.		
	<i>disable</i>	Disable NAS filter rule for RADIUS server.		
neighbor-report-dual-band	Enable/disable dual-band neighbor report (default = disable).	option	-	disable
	Option	Description		
	<i>disable</i>	Disable dual-band neighbor report.		
	<i>enable</i>	Enable dual-band neighbor report.		
okc	Enable/disable Opportunistic Key Caching (OKC) (default = enable).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable Opportunistic Key Caching (OKC).		
	<i>enable</i>	Enable Opportunistic Key Caching (OKC).		
osen	Enable/disable OSEN as part of key management (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable OSEN auth.		
	<i>disable</i>	Disable OSEN auth.		
owe-groups	OWE-Groups.	option	-	
	Option	Description		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
owe-transition	Enable/disable OWE transition mode support.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable OWE transition mode support.		
	<i>enable</i>	Enable OWE transition mode support.		

Parameter	Description	Type	Size	Default								
owe-transition-ssid	OWE transition mode peer SSID.	string	Maximum length: 32									
passphrase	WPA pre-shared key (PSK) to be used to authenticate WiFi users.	password	Not Specified									
pmf	Protected Management Frames (PMF) support (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable PMF completely.</td></tr><tr><td>enable</td><td>Enable PMF but deny clients without PMF.</td></tr><tr><td>optional</td><td>Enable PMF and allow clients without PMF.</td></tr></table>				Option	Description	disable	Disable PMF completely.	enable	Enable PMF but deny clients without PMF.	optional	Enable PMF and allow clients without PMF.
Option	Description											
disable	Disable PMF completely.											
enable	Enable PMF but deny clients without PMF.											
optional	Enable PMF and allow clients without PMF.											
pmf-assoc-comeback-timeout	Protected Management Frames (PMF) comeback maximum timeout (1-20 sec).	integer	Minimum value: 1 1 Maximum value: 20									
pmf-sa-query-retry-timeout	Protected Management Frames (PMF) SA query retry timeout interval (1 - 5 100s of msec).	integer	Minimum value: 2 1 Maximum value: 5									
port-macauth	Enable/disable LAN port MAC authentication (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable LAN port MAC authentication.</td></tr><tr><td>radius</td><td>Enable LAN port RADIUS-based MAC authentication.</td></tr><tr><td>address-group</td><td>Enable LAN port address-group based MAC authentication.</td></tr></table>				Option	Description	disable	Disable LAN port MAC authentication.	radius	Enable LAN port RADIUS-based MAC authentication.	address-group	Enable LAN port address-group based MAC authentication.
Option	Description											
disable	Disable LAN port MAC authentication.											
radius	Enable LAN port RADIUS-based MAC authentication.											
address-group	Enable LAN port address-group based MAC authentication.											
port-macauth-reauth-timeout	LAN port MAC authentication re-authentication timeout value (default = 7200 sec).	integer	Minimum value: 7200 120 Maximum value: 65535									
port-macauth-timeout	LAN port MAC authentication idle timeout value (default = 600 sec).	integer	Minimum value: 600 60 Maximum value: 65535									
portal-message-override-group	Replacement message group for this VAP (only available when security is set to a captive portal type).	string	Maximum length: 35									
portal-type	Captive portal functionality. Configure how the captive portal authenticates users and whether it includes a disclaimer.	option	-	auth								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auth</i>	Portal for authentication.		
	<i>auth+disclaimer</i>	Portal for authentication and disclaimer.		
	<i>disclaimer</i>	Portal for disclaimer.		
	<i>email-collect</i>	Portal for email collection.		
	<i>cmcc</i>	Portal for CMCC.		
	<i>cmcc-macauth</i>	Portal for CMCC and MAC authentication.		
	<i>auth-mac</i>	Portal for authentication and MAC authentication.		
	<i>external-auth</i>	Portal for external portal authentication.		
	<i>external-macauth</i>	Portal for external portal MAC authentication.		
pre-auth	Enable/disable pre-authentication, where supported by clients (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable pre-authentication.		
	<i>disable</i>	Disable pre-authentication.		
primary-wag-profile	Primary wireless access gateway profile name.	string	Maximum length: 35	
probe-resp-suppression	Enable/disable probe response suppression (to ignore weak signals) (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable probe response suppression.		
	<i>disable</i>	Disable probe response suppression.		
probe-resp-threshold	Minimum signal level/threshold in dBm required for the AP response to probe requests (-95 to -20, default = -80).	string	Maximum length: 7	-80
ptk-rekey	Enable/disable PTK rekey for WPA-Enterprise security.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PTK rekey for WPA-Enterprise security.		
	<i>disable</i>	Disable PTK rekey for WPA-Enterprise security.		

Parameter	Description	Type	Size	Default						
ptk-rekey-intv	PTK rekey interval (600 - 864000 sec, default = 86400).	integer	Minimum value: 600 Maximum value: 864000	86400						
qos-profile	Quality of service profile name.	string	Maximum length: 35							
quarantine	Enable/disable station quarantine (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable station quarantine.</td></tr><tr><td>disable</td><td>Disable station quarantine.</td></tr></table>				Option	Description	enable	Enable station quarantine.	disable	Disable station quarantine.
Option	Description									
enable	Enable station quarantine.									
disable	Disable station quarantine.									
radio-2g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 2.4G band (-95 to -20, default = -79).	string	Maximum length: 7	-79						
radio-5g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 5G band(-95 to -20, default = -76).	string	Maximum length: 7	-76						
radio-sensitivity	Enable/disable software radio sensitivity (to ignore weak signals) (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable software radio sensitivity.</td></tr><tr><td>disable</td><td>Disable software radio sensitivity.</td></tr></table>				Option	Description	enable	Enable software radio sensitivity.	disable	Disable software radio sensitivity.
Option	Description									
enable	Enable software radio sensitivity.									
disable	Disable software radio sensitivity.									
radius-mac-auth	Enable/disable RADIUS-based MAC authentication of clients (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable RADIUS-based MAC authentication.</td></tr><tr><td>disable</td><td>Disable RADIUS-based MAC authentication.</td></tr></table>				Option	Description	enable	Enable RADIUS-based MAC authentication.	disable	Disable RADIUS-based MAC authentication.
Option	Description									
enable	Enable RADIUS-based MAC authentication.									
disable	Disable RADIUS-based MAC authentication.									
radius-mac-auth-block-interval	Don't send RADIUS MAC auth request again if the client has been rejected within specific interval (0 or 30 - 864000 seconds, default = 0, 0 to disable blocking).	integer	Minimum value: 30 Maximum value: 864000	0						

Parameter	Description	Type	Size	Default																														
radius-mac-auth-server	RADIUS-based MAC authentication server.	string	Maximum length: 35																															
radius-mac-auth-usergroups <name>	Selective user groups that are permitted for RADIUS mac authentication. User group name.	string	Maximum length: 79																															
radius-mac-mpsk-auth	Enable/disable RADIUS-based MAC authentication of clients for MPSK authentication (default = disable).	option	-	disable																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RADIUS-based MAC authentication for MPSK authentication.</td></tr><tr><td><i>disable</i></td><td>Disable RADIUS-based MAC authentication for MPSK authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable RADIUS-based MAC authentication for MPSK authentication.	<i>disable</i>	Disable RADIUS-based MAC authentication for MPSK authentication.																								
Option	Description																																	
<i>enable</i>	Enable RADIUS-based MAC authentication for MPSK authentication.																																	
<i>disable</i>	Disable RADIUS-based MAC authentication for MPSK authentication.																																	
radius-mac-mpsk-timeout	RADIUS MAC MPSK cache timeout interval (0 or 300 - 864000, default = 86400, 0 to disable caching).	integer	Minimum value: 300 Maximum value: 864000	86400																														
radius-server	RADIUS server to be used to authenticate WiFi users.	string	Maximum length: 35																															
rates-11a	Allowed data rates for 802.11a.	option	-																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>6</td><td>6 Mbps supported rate.</td></tr><tr><td>6-basic</td><td>6 Mbps BSS basic rate.</td></tr><tr><td>9</td><td>9 Mbps supported rate.</td></tr><tr><td>9-basic</td><td>9 Mbps BSS basic rate.</td></tr><tr><td>12</td><td>12 Mbps supported rate.</td></tr><tr><td>12-basic</td><td>12 Mbps BSS basic rate.</td></tr><tr><td>18</td><td>18 Mbps supported rate.</td></tr><tr><td>18-basic</td><td>18 Mbps BSS basic rate.</td></tr><tr><td>24</td><td>24 Mbps supported rate.</td></tr><tr><td>24-basic</td><td>24 Mbps BSS basic rate.</td></tr><tr><td>36</td><td>36 Mbps supported rate.</td></tr><tr><td>36-basic</td><td>36 Mbps BSS basic rate.</td></tr><tr><td>48</td><td>48 Mbps supported rate.</td></tr><tr><td>48-basic</td><td>48 Mbps BSS basic rate.</td></tr></table>				Option	Description	6	6 Mbps supported rate.	6-basic	6 Mbps BSS basic rate.	9	9 Mbps supported rate.	9-basic	9 Mbps BSS basic rate.	12	12 Mbps supported rate.	12-basic	12 Mbps BSS basic rate.	18	18 Mbps supported rate.	18-basic	18 Mbps BSS basic rate.	24	24 Mbps supported rate.	24-basic	24 Mbps BSS basic rate.	36	36 Mbps supported rate.	36-basic	36 Mbps BSS basic rate.	48	48 Mbps supported rate.	48-basic	48 Mbps BSS basic rate.
Option	Description																																	
6	6 Mbps supported rate.																																	
6-basic	6 Mbps BSS basic rate.																																	
9	9 Mbps supported rate.																																	
9-basic	9 Mbps BSS basic rate.																																	
12	12 Mbps supported rate.																																	
12-basic	12 Mbps BSS basic rate.																																	
18	18 Mbps supported rate.																																	
18-basic	18 Mbps BSS basic rate.																																	
24	24 Mbps supported rate.																																	
24-basic	24 Mbps BSS basic rate.																																	
36	36 Mbps supported rate.																																	
36-basic	36 Mbps BSS basic rate.																																	
48	48 Mbps supported rate.																																	
48-basic	48 Mbps BSS basic rate.																																	

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>54</td><td>54 Mbps supported rate.</td></tr><tr><td>54-basic</td><td>54 Mbps BSS basic rate.</td></tr></table>	Option	Description	54	54 Mbps supported rate.	54-basic	54 Mbps BSS basic rate.																									
	Option	Description																														
	54	54 Mbps supported rate.																														
54-basic	54 Mbps BSS basic rate.																															
rates-11ac-mcs-map	Comma separated list of max supported VHT MCS for spatial streams 1 through 8.	string	Maximum length: 63																													
rates-11ax-mcs-map	Comma separated list of max supported HE MCS for spatial streams 1 through 8.	string	Maximum length: 63																													
rates-11be-mcs-map	Comma separated list of max nss that supports EHT-MCS 0-9, 10-11, 12-13 for 20MHz/40MHz/80MHz bandwidth.	string	Maximum length: 15																													
rates-11be-mcs-map-160	Comma separated list of max nss that supports EHT-MCS 0-9, 10-11, 12-13 for 160MHz bandwidth.	string	Maximum length: 15																													
rates-11be-mcs-map-320	Comma separated list of max nss that supports EHT-MCS 0-9, 10-11, 12-13 for 320MHz bandwidth.	string	Maximum length: 15																													
rates-11bg	Allowed data rates for 802.11b/g.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>1 Mbps supported rate.</td></tr><tr><td>1-basic</td><td>1 Mbps BSS basic rate.</td></tr><tr><td>2</td><td>2 Mbps supported rate.</td></tr><tr><td>2-basic</td><td>2 Mbps BSS basic rate.</td></tr><tr><td>5.5</td><td>5.5 Mbps supported rate.</td></tr><tr><td>5.5-basic</td><td>5.5 Mbps BSS basic rate.</td></tr><tr><td>11</td><td>11 Mbps supported rate.</td></tr><tr><td>11-basic</td><td>11 Mbps BSS basic rate.</td></tr><tr><td>6</td><td>6 Mbps supported rate.</td></tr><tr><td>6-basic</td><td>6 Mbps BSS basic rate.</td></tr><tr><td>9</td><td>9 Mbps supported rate.</td></tr><tr><td>9-basic</td><td>9 Mbps BSS basic rate.</td></tr><tr><td>12</td><td>12 Mbps supported rate.</td></tr></table>	Option	Description	1	1 Mbps supported rate.	1-basic	1 Mbps BSS basic rate.	2	2 Mbps supported rate.	2-basic	2 Mbps BSS basic rate.	5.5	5.5 Mbps supported rate.	5.5-basic	5.5 Mbps BSS basic rate.	11	11 Mbps supported rate.	11-basic	11 Mbps BSS basic rate.	6	6 Mbps supported rate.	6-basic	6 Mbps BSS basic rate.	9	9 Mbps supported rate.	9-basic	9 Mbps BSS basic rate.	12	12 Mbps supported rate.			
	Option	Description																														
	1	1 Mbps supported rate.																														
	1-basic	1 Mbps BSS basic rate.																														
	2	2 Mbps supported rate.																														
	2-basic	2 Mbps BSS basic rate.																														
	5.5	5.5 Mbps supported rate.																														
	5.5-basic	5.5 Mbps BSS basic rate.																														
	11	11 Mbps supported rate.																														
	11-basic	11 Mbps BSS basic rate.																														
	6	6 Mbps supported rate.																														
	6-basic	6 Mbps BSS basic rate.																														
	9	9 Mbps supported rate.																														
9-basic	9 Mbps BSS basic rate.																															
12	12 Mbps supported rate.																															

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>12-basic</td><td>12 Mbps BSS basic rate.</td></tr><tr><td>18</td><td>18 Mbps supported rate.</td></tr><tr><td>18-basic</td><td>18 Mbps BSS basic rate.</td></tr><tr><td>24</td><td>24 Mbps supported rate.</td></tr><tr><td>24-basic</td><td>24 Mbps BSS basic rate.</td></tr><tr><td>36</td><td>36 Mbps supported rate.</td></tr><tr><td>36-basic</td><td>36 Mbps BSS basic rate.</td></tr><tr><td>48</td><td>48 Mbps supported rate.</td></tr><tr><td>48-basic</td><td>48 Mbps BSS basic rate.</td></tr><tr><td>54</td><td>54 Mbps supported rate.</td></tr><tr><td>54-basic</td><td>54 Mbps BSS basic rate.</td></tr></table>	Option	Description	12-basic	12 Mbps BSS basic rate.	18	18 Mbps supported rate.	18-basic	18 Mbps BSS basic rate.	24	24 Mbps supported rate.	24-basic	24 Mbps BSS basic rate.	36	36 Mbps supported rate.	36-basic	36 Mbps BSS basic rate.	48	48 Mbps supported rate.	48-basic	48 Mbps BSS basic rate.	54	54 Mbps supported rate.	54-basic	54 Mbps BSS basic rate.									
	Option	Description																																
	12-basic	12 Mbps BSS basic rate.																																
	18	18 Mbps supported rate.																																
	18-basic	18 Mbps BSS basic rate.																																
	24	24 Mbps supported rate.																																
	24-basic	24 Mbps BSS basic rate.																																
	36	36 Mbps supported rate.																																
	36-basic	36 Mbps BSS basic rate.																																
	48	48 Mbps supported rate.																																
	48-basic	48 Mbps BSS basic rate.																																
	54	54 Mbps supported rate.																																
54-basic	54 Mbps BSS basic rate.																																	
rates-11n-ss12	Allowed data rates for 802.11n with 1 or 2 spatial streams.	option	-																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mcs0/1</td><td>Data rate for MCS index 0 with 1 spatial stream.</td></tr><tr><td>mcs1/1</td><td>Data rate for MCS index 1 with 1 spatial stream.</td></tr><tr><td>mcs2/1</td><td>Data rate for MCS index 2 with 1 spatial stream.</td></tr><tr><td>mcs3/1</td><td>Data rate for MCS index 3 with 1 spatial stream.</td></tr><tr><td>mcs4/1</td><td>Data rate for MCS index 4 with 1 spatial stream.</td></tr><tr><td>mcs5/1</td><td>Data rate for MCS index 5 with 1 spatial stream.</td></tr><tr><td>mcs6/1</td><td>Data rate for MCS index 6 with 1 spatial stream.</td></tr><tr><td>mcs7/1</td><td>Data rate for MCS index 7 with 1 spatial stream.</td></tr><tr><td>mcs8/2</td><td>Data rate for MCS index 8 with 2 spatial streams.</td></tr><tr><td>mcs9/2</td><td>Data rate for MCS index 9 with 2 spatial streams.</td></tr><tr><td>mcs10/2</td><td>Data rate for MCS index 10 with 2 spatial streams.</td></tr><tr><td>mcs11/2</td><td>Data rate for MCS index 11 with 2 spatial streams.</td></tr><tr><td>mcs12/2</td><td>Data rate for MCS index 12 with 2 spatial streams.</td></tr><tr><td>mcs13/2</td><td>Data rate for MCS index 13 with 2 spatial streams.</td></tr></table>	Option	Description	mcs0/1	Data rate for MCS index 0 with 1 spatial stream.	mcs1/1	Data rate for MCS index 1 with 1 spatial stream.	mcs2/1	Data rate for MCS index 2 with 1 spatial stream.	mcs3/1	Data rate for MCS index 3 with 1 spatial stream.	mcs4/1	Data rate for MCS index 4 with 1 spatial stream.	mcs5/1	Data rate for MCS index 5 with 1 spatial stream.	mcs6/1	Data rate for MCS index 6 with 1 spatial stream.	mcs7/1	Data rate for MCS index 7 with 1 spatial stream.	mcs8/2	Data rate for MCS index 8 with 2 spatial streams.	mcs9/2	Data rate for MCS index 9 with 2 spatial streams.	mcs10/2	Data rate for MCS index 10 with 2 spatial streams.	mcs11/2	Data rate for MCS index 11 with 2 spatial streams.	mcs12/2	Data rate for MCS index 12 with 2 spatial streams.	mcs13/2	Data rate for MCS index 13 with 2 spatial streams.			
	Option	Description																																
	mcs0/1	Data rate for MCS index 0 with 1 spatial stream.																																
	mcs1/1	Data rate for MCS index 1 with 1 spatial stream.																																
	mcs2/1	Data rate for MCS index 2 with 1 spatial stream.																																
	mcs3/1	Data rate for MCS index 3 with 1 spatial stream.																																
	mcs4/1	Data rate for MCS index 4 with 1 spatial stream.																																
	mcs5/1	Data rate for MCS index 5 with 1 spatial stream.																																
	mcs6/1	Data rate for MCS index 6 with 1 spatial stream.																																
	mcs7/1	Data rate for MCS index 7 with 1 spatial stream.																																
	mcs8/2	Data rate for MCS index 8 with 2 spatial streams.																																
	mcs9/2	Data rate for MCS index 9 with 2 spatial streams.																																
	mcs10/2	Data rate for MCS index 10 with 2 spatial streams.																																
	mcs11/2	Data rate for MCS index 11 with 2 spatial streams.																																
mcs12/2	Data rate for MCS index 12 with 2 spatial streams.																																	
mcs13/2	Data rate for MCS index 13 with 2 spatial streams.																																	

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mcs14/2</td><td>Data rate for MCS index 14 with 2 spatial streams.</td></tr><tr><td>mcs15/2</td><td>Data rate for MCS index 15 with 2 spatial streams.</td></tr></table>	Option	Description	mcs14/2	Data rate for MCS index 14 with 2 spatial streams.	mcs15/2	Data rate for MCS index 15 with 2 spatial streams.																															
	Option	Description																																				
	mcs14/2	Data rate for MCS index 14 with 2 spatial streams.																																				
mcs15/2	Data rate for MCS index 15 with 2 spatial streams.																																					
rates-11n-ss34	Allowed data rates for 802.11n with 3 or 4 spatial streams.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mcs16/3</td><td>Data rate for MCS index 16 with 3 spatial streams.</td></tr><tr><td>mcs17/3</td><td>Data rate for MCS index 17 with 3 spatial streams.</td></tr><tr><td>mcs18/3</td><td>Data rate for MCS index 18 with 3 spatial streams.</td></tr><tr><td>mcs19/3</td><td>Data rate for MCS index 19 with 3 spatial streams.</td></tr><tr><td>mcs20/3</td><td>Data rate for MCS index 20 with 3 spatial streams.</td></tr><tr><td>mcs21/3</td><td>Data rate for MCS index 21 with 3 spatial streams.</td></tr><tr><td>mcs22/3</td><td>Data rate for MCS index 22 with 3 spatial streams.</td></tr><tr><td>mcs23/3</td><td>Data rate for MCS index 23 with 3 spatial streams.</td></tr><tr><td>mcs24/4</td><td>Data rate for MCS index 24 with 4 spatial streams.</td></tr><tr><td>mcs25/4</td><td>Data rate for MCS index 25 with 4 spatial streams.</td></tr><tr><td>mcs26/4</td><td>Data rate for MCS index 26 with 4 spatial streams.</td></tr><tr><td>mcs27/4</td><td>Data rate for MCS index 27 with 4 spatial streams.</td></tr><tr><td>mcs28/4</td><td>Data rate for MCS index 28 with 4 spatial streams.</td></tr><tr><td>mcs29/4</td><td>Data rate for MCS index 29 with 4 spatial streams.</td></tr><tr><td>mcs30/4</td><td>Data rate for MCS index 30 with 4 spatial streams.</td></tr><tr><td>mcs31/4</td><td>Data rate for MCS index 31 with 4 spatial streams.</td></tr></table>	Option	Description	mcs16/3	Data rate for MCS index 16 with 3 spatial streams.	mcs17/3	Data rate for MCS index 17 with 3 spatial streams.	mcs18/3	Data rate for MCS index 18 with 3 spatial streams.	mcs19/3	Data rate for MCS index 19 with 3 spatial streams.	mcs20/3	Data rate for MCS index 20 with 3 spatial streams.	mcs21/3	Data rate for MCS index 21 with 3 spatial streams.	mcs22/3	Data rate for MCS index 22 with 3 spatial streams.	mcs23/3	Data rate for MCS index 23 with 3 spatial streams.	mcs24/4	Data rate for MCS index 24 with 4 spatial streams.	mcs25/4	Data rate for MCS index 25 with 4 spatial streams.	mcs26/4	Data rate for MCS index 26 with 4 spatial streams.	mcs27/4	Data rate for MCS index 27 with 4 spatial streams.	mcs28/4	Data rate for MCS index 28 with 4 spatial streams.	mcs29/4	Data rate for MCS index 29 with 4 spatial streams.	mcs30/4	Data rate for MCS index 30 with 4 spatial streams.	mcs31/4	Data rate for MCS index 31 with 4 spatial streams.			
	Option	Description																																				
	mcs16/3	Data rate for MCS index 16 with 3 spatial streams.																																				
	mcs17/3	Data rate for MCS index 17 with 3 spatial streams.																																				
	mcs18/3	Data rate for MCS index 18 with 3 spatial streams.																																				
	mcs19/3	Data rate for MCS index 19 with 3 spatial streams.																																				
	mcs20/3	Data rate for MCS index 20 with 3 spatial streams.																																				
	mcs21/3	Data rate for MCS index 21 with 3 spatial streams.																																				
	mcs22/3	Data rate for MCS index 22 with 3 spatial streams.																																				
	mcs23/3	Data rate for MCS index 23 with 3 spatial streams.																																				
	mcs24/4	Data rate for MCS index 24 with 4 spatial streams.																																				
	mcs25/4	Data rate for MCS index 25 with 4 spatial streams.																																				
	mcs26/4	Data rate for MCS index 26 with 4 spatial streams.																																				
	mcs27/4	Data rate for MCS index 27 with 4 spatial streams.																																				
	mcs28/4	Data rate for MCS index 28 with 4 spatial streams.																																				
	mcs29/4	Data rate for MCS index 29 with 4 spatial streams.																																				
mcs30/4	Data rate for MCS index 30 with 4 spatial streams.																																					
mcs31/4	Data rate for MCS index 31 with 4 spatial streams.																																					
roaming-acct-interim-update	Enable/disable using accounting interim update instead of accounting start/stop on roaming for WPA-Enterprise security.	option	-	disable																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable using accounting interim update on roaming for WPA-Enterprise security.</td></tr><tr><td>disable</td><td>Disable using accounting interim update on roaming for WPA-Enterprise security.</td></tr></table>	Option	Description	enable	Enable using accounting interim update on roaming for WPA-Enterprise security.	disable	Disable using accounting interim update on roaming for WPA-Enterprise security.																															
	Option	Description																																				
	enable	Enable using accounting interim update on roaming for WPA-Enterprise security.																																				
disable	Disable using accounting interim update on roaming for WPA-Enterprise security.																																					
sae-groups	SAE-Groups.	option	-																																			

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr></table>	Option	Description	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.			
	Option	Description										
	19	DH Group 19.										
	20	DH Group 20.										
21	DH Group 21.											
sae-h2e-only	Use hash-to-element-only mechanism for PWE derivation (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WPA3 SAE-H2E-only.</td></tr><tr><td>disable</td><td>Disable WPA3 SAE-H2E-only.</td></tr></table>	Option	Description	enable	Enable WPA3 SAE-H2E-only.	disable	Disable WPA3 SAE-H2E-only.					
	Option	Description										
	enable	Enable WPA3 SAE-H2E-only.										
disable	Disable WPA3 SAE-H2E-only.											
sae-hnp-only	Use hunting-and-pecking-only mechanism for PWE derivation (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WPA3 SAE-HNP-only.</td></tr><tr><td>disable</td><td>Disable WPA3 SAE-HNP-only.</td></tr></table>	Option	Description	enable	Enable WPA3 SAE-HNP-only.	disable	Disable WPA3 SAE-HNP-only.					
	Option	Description										
	enable	Enable WPA3 SAE-HNP-only.										
disable	Disable WPA3 SAE-HNP-only.											
sae-password	WPA3 SAE password to be used to authenticate WiFi users.	password	Not Specified									
sae-pk	Enable/disable WPA3 SAE-PK (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WPA3 SAE-PK.</td></tr><tr><td>disable</td><td>Disable WPA3 SAE-PK.</td></tr></table>	Option	Description	enable	Enable WPA3 SAE-PK.	disable	Disable WPA3 SAE-PK.					
	Option	Description										
	enable	Enable WPA3 SAE-PK.										
disable	Disable WPA3 SAE-PK.											
sae-private-key	Private key used for WPA3 SAE-PK authentication.	string	Maximum length: 359									
scan-botnet-connections	Block or monitor connections to Botnet servers or disable Botnet scanning.	option	-	monitor								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not scan connections to botnet servers.</td></tr><tr><td>monitor</td><td>Log connections to botnet servers.</td></tr><tr><td>block</td><td>Block connections to botnet servers.</td></tr></table>	Option	Description	disable	Do not scan connections to botnet servers.	monitor	Log connections to botnet servers.	block	Block connections to botnet servers.			
	Option	Description										
	disable	Do not scan connections to botnet servers.										
	monitor	Log connections to botnet servers.										
block	Block connections to botnet servers.											

Parameter	Description	Type	Size	Default
schedule <name>	Firewall schedules for enabling this VAP on the FortiAP. This VAP will be enabled when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35	
secondary-wag-profile	Secondary wireless access gateway profile name.	string	Maximum length: 35	
security	Security mode for the wireless interface (default = wpa2-only-personal).	option	-	wpa2-only-personal

Option	Description
<i>open</i>	Open.
<i>wep64</i>	WEP 64-bit.
<i>wep128</i>	WEP 128-bit.
<i>wpa-personal</i>	WPA/WPA2 personal.
<i>wpa-enterprise</i>	WPA/WPA2 enterprise.
<i>wpa-only-personal</i>	WPA personal.
<i>wpa-only-enterprise</i>	WPA enterprise.
<i>wpa2-only-personal</i>	WPA2 personal.
<i>wpa2-only-enterprise</i>	WPA2 enterprise.
<i>wpa3-enterprise</i>	WPA3 enterprise with 192-bit encryption and PMF mandatory.
<i>wpa3-only-enterprise</i>	WPA3 enterprise with PMF mandatory.
<i>wpa3-enterprise-transition</i>	WPA3 enterprise with PMF optional.
<i>wpa3-sae</i>	WPA3 SAE.
<i>wpa3-sae-transition</i>	WPA3 SAE transition.
<i>owe</i>	Opportunistic wireless encryption.
<i>osen</i>	OSEN.

Parameter	Description	Type	Size	Default						
security-exempt-list	Optional security exempt list for captive portal authentication.	string	Maximum length: 35							
security-redirect-url	Optional URL for redirecting users after they pass captive portal authentication.	var-string	Maximum length: 1023							
selected-usergroups<name>	Selective user groups that are permitted to authenticate. User group name.	string	Maximum length: 79							
split-tunneling	Enable/disable split tunneling (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable split tunneling.</td></tr><tr><td>disable</td><td>Disable split tunneling.</td></tr></table>	Option	Description	enable	Enable split tunneling.	disable	Disable split tunneling.			
Option	Description									
enable	Enable split tunneling.									
disable	Disable split tunneling.									
ssid	IEEE 802.11 service set identifier (SSID) for the wireless interface. Users who wish to use the wireless network must configure their computers to access this SSID name.	string	Maximum length: 32	fortinet						
sticky-client-remove	Enable/disable sticky client remove to maintain good signal level clients in SSID (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sticky client remove.</td></tr><tr><td>disable</td><td>Disable sticky client remove.</td></tr></table>	Option	Description	enable	Enable sticky client remove.	disable	Disable sticky client remove.			
Option	Description									
enable	Enable sticky client remove.									
disable	Disable sticky client remove.									
sticky-client-threshold-2g	Minimum signal level/threshold in dBm required for the 2G client to be serviced by the AP (-95 to -20, default = -79).	string	Maximum length: 7	-79						
sticky-client-threshold-5g	Minimum signal level/threshold in dBm required for the 5G client to be serviced by the AP (-95 to -20, default = -76).	string	Maximum length: 7	-76						
sticky-client-threshold-6g	Minimum signal level/threshold in dBm required for the 6G client to be serviced by the AP (-95 to -20, default = -76).	string	Maximum length: 7	-76						
target-wake-time	Enable/disable 802.11ax target wake time (default = enable).	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable 802.11ax target wake time.		
	<i>disable</i>	Disable 802.11ax target wake time.		
tkip-counter-measure	Enable/disable TKIP counter measure.	option	-	enable
	Option Description			
	<i>enable</i>	Enable TKIP counter measure.		
	<i>disable</i>	Disable TKIP counter measure.		
tunnel-echo-interval	The time interval to send echo to both primary and secondary tunnel peers (1 - 65535 sec, default = 300).	integer	Minimum value: 300 1 Maximum value: 65535	
tunnel-fallback-interval	The time interval for secondary tunnel to fall back to primary tunnel (0 - 65535 sec, default = 7200).	integer	Minimum value: 7200 0 Maximum value: 65535	
usergroup <name>	Firewall user group to be used to authenticate WiFi users. User group name.	string	Maximum length: 79	
utm-log	Enable/disable UTM logging.	option	-	enable
	Option Description			
	<i>enable</i>	Enable UTM logging.		
	<i>disable</i>	Disable UTM logging.		
utm-profile	UTM profile name.	string	Maximum length: 35	
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the VAP.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
vlan-auto	Enable/disable automatic management of SSID VLAN interface.	option	-	disable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic management of SSID VLAN interface.</td></tr><tr><td><i>disable</i></td><td>Disable automatic management of SSID VLAN interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic management of SSID VLAN interface.	<i>disable</i>	Disable automatic management of SSID VLAN interface.							
	Option	Description												
	<i>enable</i>	Enable automatic management of SSID VLAN interface.												
<i>disable</i>	Disable automatic management of SSID VLAN interface.													
vlan-pooling	Enable/disable VLAN pooling, to allow grouping of multiple wireless controller VLANs into VLAN pools (default = disable). When set to wtp-group, VLAN pooling occurs with VLAN assignment by wtp-group.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wtp-group</i></td><td>Enable VLAN pooling with VLAN assignment by wtp-group.</td></tr><tr><td><i>round-robin</i></td><td>Enable VLAN pooling with round-robin VLAN assignment.</td></tr><tr><td><i>hash</i></td><td>Enable VLAN pooling with hash-based VLAN assignment.</td></tr><tr><td><i>disable</i></td><td>Disable VLAN pooling.</td></tr></table>	Option	Description	<i>wtp-group</i>	Enable VLAN pooling with VLAN assignment by wtp-group.	<i>round-robin</i>	Enable VLAN pooling with round-robin VLAN assignment.	<i>hash</i>	Enable VLAN pooling with hash-based VLAN assignment.	<i>disable</i>	Disable VLAN pooling.			
	Option	Description												
	<i>wtp-group</i>	Enable VLAN pooling with VLAN assignment by wtp-group.												
	<i>round-robin</i>	Enable VLAN pooling with round-robin VLAN assignment.												
	<i>hash</i>	Enable VLAN pooling with hash-based VLAN assignment.												
<i>disable</i>	Disable VLAN pooling.													
vlanid	Optional VLAN ID.	integer	Minimum value: 0 Maximum value: 4094											
webfilter-profile	WebFilter profile name.	string	Maximum length: 47											

config portal-message-overrides

Parameter	Description	Type	Size	Default
auth-disclaimer-page	Override auth-disclaimer-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-login-failed-page	Override auth-login-failed-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-login-page	Override auth-login-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-reject-page	Override auth-reject-page message with message from portal-message-overrides group.	string	Maximum length: 35	

config vlan-name

Parameter	Description	Type	Size	Default
name	VLAN name.	string	Maximum length: 35	
vlan-id	VLAN IDs (maximum 8 VLAN IDs).	integer	Minimum value: 0 Maximum value: 4094	

config vlan-pool

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4094	0
wtp-group	WTP group name.	string	Maximum length: 35	

config wireless-controller vap-group

Configure virtual Access Point (VAP) groups.

```
config wireless-controller vap-group
  Description: Configure virtual Access Point (VAP) groups.
  edit <name>
    set comment {var-string}
    set vaps <name1>, <name2>, ...
  next
end
```

config wireless-controller vap-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Group Name.	string	Maximum length: 35	
vaps <name>	List of SSIDs to be included in the VAP group. VAP name.	string	Maximum length: 35	

config wireless-controller wag-profile

Configure wireless access gateway (WAG) profiles used for tunnels on AP.

```
config wireless-controller wag-profile
  Description: Configure wireless access gateway (WAG) profiles used for tunnels on AP.
  edit <name>
    set comment {var-string}
    set dhcp-ip-addr {ipv4-address}
    set ping-interval {integer}
    set ping-number {integer}
    set return-packet-timeout {integer}
    set tunnel-type [l2tpv3|gre]
    set wag-ip {ipv4-address}
    set wag-port {integer}
  next
end
```

config wireless-controller wag-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
dhcp-ip-addr	IP address of the monitoring DHCP request packet sent through the tunnel.	ipv4-address	Not Specified	0.0.0.0
name	Tunnel profile name.	string	Maximum length: 35	
ping-interval	Interval between two tunnel monitoring echo packets (1 - 65535 sec, default = 1).	integer	Minimum value: 1 Maximum value: 65535	1
ping-number	Number of the tunnel monitoring echo packets (1 - 65535, default = 5).	integer	Minimum value: 1 Maximum value: 65535	5
return-packet-timeout	Window of time for the return packets from the tunnel's remote end (1 - 65535 sec, default = 160).	integer	Minimum value: 1 Maximum value: 65535	160
tunnel-type	Tunnel type.	option	-	l2tpv3

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>l2tpv3</i>	L2TPV3 Ethernet Pseudowire.		
	<i>gre</i>	GRE Ethernet tunnel.		
wag-ip	IP Address of the wireless access gateway.	ipv4-address	Not Specified	0.0.0.0
wag-port	UDP port of the wireless access gateway.	integer	Minimum value: 0 Maximum value: 65535	1701

config wireless-controller wids-profile

Configure wireless intrusion detection system (WIDS) profiles.

```

config wireless-controller wids-profile
  Description: Configure wireless intrusion detection system (WIDS) profiles.
  edit <name>
    set adhoc-network [enable|disable]
    set adhoc-valid-ssid [enable|disable]
    set air-jack [enable|disable]
    set ap-auto-suppress [enable|disable]
    set ap-bgscan-disable-schedules <name1>, <name2>, ...
    set ap-bgscan-duration {integer}
    set ap-bgscan-idle {integer}
    set ap-bgscan-intv {integer}
    set ap-bgscan-period {integer}
    set ap-bgscan-report-intv {integer}
    set ap-fgscan-report-intv {integer}
    set ap-impersonation [enable|disable]
    set ap-scan [disable|enable]
    set ap-scan-channel-list-2G-5G <chan1>, <chan2>, ...
    set ap-scan-channel-list-6G <chan1>, <chan2>, ...
    set ap-scan-passive [enable|disable]
    set ap-scan-threshold {string}
    set ap-spoofing [enable|disable]
    set asleap-attack [enable|disable]
    set assoc-flood-thresh {integer}
    set assoc-flood-time {integer}
    set assoc-frame-flood [enable|disable]
    set auth-flood-thresh {integer}
    set auth-flood-time {integer}
    set auth-frame-flood [enable|disable]
    set bcn-flood [enable|disable]
    set bcn-flood-thresh {integer}

```

```
set bcn-flood-time {integer}
set beacon-wrong-channel [enable|disable]
set block_ack-flood [enable|disable]
set block_ack-flood-thresh {integer}
set block_ack-flood-time {integer}
set chan-based-mitm [enable|disable]
set client-flood [enable|disable]
set client-flood-thresh {integer}
set client-flood-time {integer}
set comment {string}
set cts-flood [enable|disable]
set cts-flood-thresh {integer}
set cts-flood-time {integer}
set deauth-broadcast [enable|disable]
set deauth-unknown-src-thresh {integer}
set disassoc-broadcast [enable|disable]
set disconnect-station [enable|disable]
set eapol-fail-flood [enable|disable]
set eapol-fail-intv {integer}
set eapol-fail-thresh {integer}
set eapol-key-overflow [enable|disable]
set eapol-logoff-flood [enable|disable]
set eapol-logoff-intv {integer}
set eapol-logoff-thresh {integer}
set eapol-pre-fail-flood [enable|disable]
set eapol-pre-fail-intv {integer}
set eapol-pre-fail-thresh {integer}
set eapol-pre-succ-flood [enable|disable]
set eapol-pre-succ-intv {integer}
set eapol-pre-succ-thresh {integer}
set eapol-start-flood [enable|disable]
set eapol-start-intv {integer}
set eapol-start-thresh {integer}
set eapol-succ-flood [enable|disable]
set eapol-succ-intv {integer}
set eapol-succ-thresh {integer}
set fata-jack [enable|disable]
set fuzzed-beacon [enable|disable]
set fuzzed-probe-request [enable|disable]
set fuzzed-probe-response [enable|disable]
set hotspotter-attack [enable|disable]
set ht-40mhz-intolerance [enable|disable]
set ht-greenfield [enable|disable]
set invalid-addr-combination [enable|disable]
set invalid-mac-oui [enable|disable]
set long-duration-attack [enable|disable]
set long-duration-thresh {integer}
set malformed-association [enable|disable]
set malformed-auth [enable|disable]
set malformed-ht-ie [enable|disable]
set netstumbler [enable|disable]
set netstumbler-thresh {integer}
```

```

set netstumbler-time {integer}
set null-ssid-probe-resp [enable|disable]
set omerta-attack [enable|disable]
set overflow-ie [enable|disable]
set probe-flood [enable|disable]
set probe-flood-thresh {integer}
set probe-flood-time {integer}
set pspoll-flood [enable|disable]
set pspoll-flood-thresh {integer}
set pspoll-flood-time {integer}
set pwsave-dos-attack [enable|disable]
set reassoc-flood [enable|disable]
set reassoc-flood-thresh {integer}
set reassoc-flood-time {integer}
set risky-encryption [enable|disable]
set rts-flood [enable|disable]
set rts-flood-thresh {integer}
set rts-flood-time {integer}
set sensor-mode [disable|foreign|...]
set spoofed-deauth [enable|disable]
set unencrypted-valid [enable|disable]
set valid-client-misassociation [enable|disable]
set valid-ssid-misuse [enable|disable]
set weak-wep-iv [enable|disable]
set wellenreiter [enable|disable]
set wellenreiter-thresh {integer}
set wellenreiter-time {integer}
set windows-bridge [enable|disable]
set wireless-bridge [enable|disable]
set wpa-ft-attack [enable|disable]
next
end

```

config wireless-controller wids-profile

Parameter	Description	Type	Size	Default
adhoc-network	Enable/disable adhoc network detection (default = disable).	option	-	disable
	Option	Description		
	enable	Enable adhoc network detection.		
	disable	Disable adhoc network detection.		
adhoc-valid-ssid	Enable/disable adhoc using valid SSID detection (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adhoc using valid SSID detection.</td></tr><tr><td><i>disable</i></td><td>Disable adhoc using valid SSID detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable adhoc using valid SSID detection.	<i>disable</i>	Disable adhoc using valid SSID detection.			
	Option	Description								
	<i>enable</i>	Enable adhoc using valid SSID detection.								
<i>disable</i>	Disable adhoc using valid SSID detection.									
air-jack	Enable/disable AirJack detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AirJack detection.</td></tr><tr><td><i>disable</i></td><td>Disable AirJack detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable AirJack detection.	<i>disable</i>	Disable AirJack detection.			
	Option	Description								
	<i>enable</i>	Enable AirJack detection.								
<i>disable</i>	Disable AirJack detection.									
ap-auto-suppress	Enable/disable on-wire rogue AP auto-suppression (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable on-wire rogue AP auto-suppression.</td></tr><tr><td><i>disable</i></td><td>Disable on-wire rogue AP auto-suppression.</td></tr></table>	Option	Description	<i>enable</i>	Enable on-wire rogue AP auto-suppression.	<i>disable</i>	Disable on-wire rogue AP auto-suppression.			
	Option	Description								
	<i>enable</i>	Enable on-wire rogue AP auto-suppression.								
<i>disable</i>	Disable on-wire rogue AP auto-suppression.									
ap-bgscan-disable-schedules <name>	Firewall schedules for turning off FortiAP radio background scan. Background scan will be disabled when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35							
ap-bgscan-duration	Listen time on scanning a channel (10 - 1000 msec, default = 30).	integer	Minimum value: 10 Maximum value: 1000	30						
ap-bgscan-idle	Wait time for channel inactivity before scanning this channel (0 - 1000 msec, default = 20).	integer	Minimum value: 0 Maximum value: 1000	20						
ap-bgscan-intv	Period between successive channel scans (1 - 600 sec, default = 3).	integer	Minimum value: 1 Maximum value: 600	3						
ap-bgscan-period	Period between background scans (10 - 3600 sec, default = 600).	integer	Minimum value: 10 Maximum value: 3600	600						

Parameter	Description	Type	Size	Default						
ap-bgscan-report-intv	Period between background scan reports (15 - 600 sec, default = 30).	integer	Minimum value: 15 Maximum value: 600	30						
ap-fgscan-report-intv	Period between foreground scan reports (15 - 600 sec, default = 15).	integer	Minimum value: 15 Maximum value: 600	15						
ap-impersonation	Enable/disable AP impersonation detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP impersonation detection.</td></tr><tr><td><i>disable</i></td><td>Disable AP impersonation detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP impersonation detection.	<i>disable</i>	Disable AP impersonation detection.			
Option	Description									
<i>enable</i>	Enable AP impersonation detection.									
<i>disable</i>	Disable AP impersonation detection.									
ap-scan	Enable/disable rogue AP detection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable rogue AP detection.</td></tr><tr><td><i>enable</i></td><td>Enable rogue AP detection.</td></tr></table>	Option	Description	<i>disable</i>	Disable rogue AP detection.	<i>enable</i>	Enable rogue AP detection.			
Option	Description									
<i>disable</i>	Disable rogue AP detection.									
<i>enable</i>	Enable rogue AP detection.									
ap-scan-channel-list-2G-5G <chan>	Selected ap scan channel list for 2.4G and 5G bands. Channel number.	string	Maximum length: 3							
ap-scan-channel-list-6G <chan>	Selected ap scan channel list for 6G band. Channel 6g number.	string	Maximum length: 3							
ap-scan-passive	Enable/disable passive scanning. Enable means do not send probe request on any channels (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Passive scanning on all channels.</td></tr><tr><td><i>disable</i></td><td>Passive scanning only on DFS channels.</td></tr></table>	Option	Description	<i>enable</i>	Passive scanning on all channels.	<i>disable</i>	Passive scanning only on DFS channels.			
Option	Description									
<i>enable</i>	Passive scanning on all channels.									
<i>disable</i>	Passive scanning only on DFS channels.									
ap-scan-threshold	Minimum signal level/threshold in dBm required for the AP to report detected rogue AP (-95 to -20, default = -90).	string	Maximum length: 7	-90						
ap-spoofing	Enable/disable AP spoofing detection (default = disable).	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable AP spoofing detection.		
	<i>disable</i>	Disable AP spoofing detection.		
asleep-attack	Enable/disable asleep attack detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable asleep attack detection.		
	<i>disable</i>	Disable asleep attack detection.		
assoc-flood-thresh	The threshold value for association frame flooding.	integer	Minimum value: 1 Maximum value: 100	30
assoc-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120	10
assoc-frame-flood	Enable/disable association frame flooding detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable association frame flooding detection.		
	<i>disable</i>	Disable association frame flooding detection.		
auth-flood-thresh	The threshold value for authentication frame flooding.	integer	Minimum value: 1 Maximum value: 100	30
auth-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120	10
auth-frame-flood	Enable/disable authentication frame flooding detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable authentication frame flooding detection.		
	<i>disable</i>	Disable authentication frame flooding detection.		

Parameter	Description	Type	Size	Default
bcn-flood	Enable/disable bcn flood detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable bcn flood detection.		
	<i>disable</i>	Disable bcn flood detection.		
bcn-flood-thresh	The threshold value for bcn flood.	integer	Minimum value: 1 Maximum value: 65100	15
bcn-flood-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	1
beacon-wrong-channel	Enable/disable beacon wrong channel detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable beacon wrong channel detection.		
	<i>disable</i>	Disable beacon wrong channel detection.		
block_ack-flood	Enable/disable block_ack flood detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable block_ack flood detection.		
	<i>disable</i>	Disable block_ack flood detection.		
block_ack-flood-thresh	The threshold value for block_ack flood.	integer	Minimum value: 1 Maximum value: 65100	50
block_ack-flood-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	1
chan-based-mitm	Enable/disable channel based mitm detection (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable channel based mitm detection.</td></tr><tr><td><i>disable</i></td><td>Disable channel based mitm detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable channel based mitm detection.	<i>disable</i>	Disable channel based mitm detection.			
	Option	Description								
	<i>enable</i>	Enable channel based mitm detection.								
<i>disable</i>	Disable channel based mitm detection.									
client-flood	Enable/disable client flood detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable client flood detection.</td></tr><tr><td><i>disable</i></td><td>Disable client flood detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable client flood detection.	<i>disable</i>	Disable client flood detection.			
	Option	Description								
	<i>enable</i>	Enable client flood detection.								
<i>disable</i>	Disable client flood detection.									
client-flood-thresh	The threshold value for client flood.	integer	Minimum value: 1 Maximum value: 65100	30						
client-flood-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	10						
comment	Comment.	string	Maximum length: 63							
cts-flood	Enable/disable cts flood detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable cts flood detection.</td></tr><tr><td><i>disable</i></td><td>Disable cts flood detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable cts flood detection.	<i>disable</i>	Disable cts flood detection.			
	Option	Description								
	<i>enable</i>	Enable cts flood detection.								
<i>disable</i>	Disable cts flood detection.									
cts-flood-thresh	The threshold value for cts flood.	integer	Minimum value: 1 Maximum value: 65100	30						
cts-flood-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	10						
death-broadcast	Enable/disable broadcasting de-authentication detection (default = disable).	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcast de-authentication detection.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast de-authentication detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcast de-authentication detection.	<i>disable</i>	Disable broadcast de-authentication detection.			
	Option	Description								
	<i>enable</i>	Enable broadcast de-authentication detection.								
<i>disable</i>	Disable broadcast de-authentication detection.									
deauth-unknown-src-thresh	Threshold value per second to deauth unknown src for DoS attack (0: no limit).	integer	Minimum value: 0 Maximum value: 65535	10						
disassoc-broadcast	Enable/disable broadcast dis-association detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcast dis-association detection.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast dis-association detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcast dis-association detection.	<i>disable</i>	Disable broadcast dis-association detection.			
	Option	Description								
	<i>enable</i>	Enable broadcast dis-association detection.								
<i>disable</i>	Disable broadcast dis-association detection.									
disconnect-station	Enable/disable disconnect station detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable disconnect station detection.</td></tr><tr><td><i>disable</i></td><td>Disable disconnect station detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable disconnect station detection.	<i>disable</i>	Disable disconnect station detection.			
	Option	Description								
	<i>enable</i>	Enable disconnect station detection.								
<i>disable</i>	Disable disconnect station detection.									
eapol-fail-flood	Enable/disable EAPOL-Failure flooding (to AP) detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAPOL-Failure flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable EAPOL-Failure flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAPOL-Failure flooding detection.	<i>disable</i>	Disable EAPOL-Failure flooding detection.			
	Option	Description								
	<i>enable</i>	Enable EAPOL-Failure flooding detection.								
<i>disable</i>	Disable EAPOL-Failure flooding detection.									
eapol-fail-intv	The detection interval for EAPOL-Failure flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600	1						
eapol-fail-thresh	The threshold value for EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
eapol-key-overflow	Enable/disable overflow EAPOL key detection (default = disable).	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable overflow EAPOL key detection.</td></tr><tr><td><i>disable</i></td><td>Disable overflow EAPOL key detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable overflow EAPOL key detection.	<i>disable</i>	Disable overflow EAPOL key detection.			
	Option	Description								
	<i>enable</i>	Enable overflow EAPOL key detection.								
<i>disable</i>	Disable overflow EAPOL key detection.									
eapol-logoff-flood	Enable/disable EAPOL-Logoff flooding (to AP) detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAPOL-Logoff flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable EAPOL-Logoff flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAPOL-Logoff flooding detection.	<i>disable</i>	Disable EAPOL-Logoff flooding detection.			
	Option	Description								
	<i>enable</i>	Enable EAPOL-Logoff flooding detection.								
<i>disable</i>	Disable EAPOL-Logoff flooding detection.									
eapol-logoff-intv	The detection interval for EAPOL-Logoff flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600	1						
eapol-logoff-thresh	The threshold value for EAPOL-Logoff flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
eapol-pre-fail-flood	Enable/disable premature EAPOL-Failure flooding (to STA) detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable premature EAPOL-Failure flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable premature EAPOL-Failure flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable premature EAPOL-Failure flooding detection.	<i>disable</i>	Disable premature EAPOL-Failure flooding detection.			
	Option	Description								
	<i>enable</i>	Enable premature EAPOL-Failure flooding detection.								
<i>disable</i>	Disable premature EAPOL-Failure flooding detection.									
eapol-pre-fail-intv	The detection interval for premature EAPOL-Failure flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600	1						
eapol-pre-fail-thresh	The threshold value for premature EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
eapol-pre-succ-flood	Enable/disable premature EAPOL-Success flooding (to STA) detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable premature EAPOL-Success flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable premature EAPOL-Success flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable premature EAPOL-Success flooding detection.	<i>disable</i>	Disable premature EAPOL-Success flooding detection.			
	Option	Description								
	<i>enable</i>	Enable premature EAPOL-Success flooding detection.								
<i>disable</i>	Disable premature EAPOL-Success flooding detection.									

Parameter	Description	Type	Size	Default
eapol-pre-succ-intv	The detection interval for premature EAPOL-Success flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600	1
eapol-pre-succ-thresh	The threshold value for premature EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
eapol-start-flood	Enable/disable EAPOL-Start flooding (to AP) detection (default = disable).	option	-	disable
	Option	Description		
	enable	Enable EAPOL-Start flooding detection.		
	disable	Disable EAPOL-Start flooding detection.		
eapol-start-intv	The detection interval for EAPOL-Start flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600	1
eapol-start-thresh	The threshold value for EAPOL-Start flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
eapol-succ-flood	Enable/disable EAPOL-Success flooding (to AP) detection (default = disable).	option	-	disable
	Option	Description		
	enable	Enable EAPOL-Success flooding detection.		
	disable	Disable EAPOL-Success flooding detection.		
eapol-succ-intv	The detection interval for EAPOL-Success flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600	1
eapol-succ-thresh	The threshold value for EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
fata-jack	Enable/disable FATA-Jack detection (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable FATA-Jack detection.		
	<i>disable</i>	Disable FATA-Jack detection.		
fuzzed-beacon	Enable/disable fuzzed beacon detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable fuzzed beacon detection.		
	<i>disable</i>	Disable fuzzed beacon detection.		
fuzzed-probe-request	Enable/disable fuzzed probe request detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable fuzzed probe request detection.		
	<i>disable</i>	Disable fuzzed probe request detection.		
fuzzed-probe-response	Enable/disable fuzzed probe response detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable fuzzed probe response detection.		
	<i>disable</i>	Disable fuzzed probe response detection.		
hotspotter-attack	Enable/disable hotspotter attack detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable hotspotter attack detection.		
	<i>disable</i>	Disable hotspotter attack detection.		
ht-40mhz-intolerance	Enable/disable HT 40 MHz intolerance detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HT 40 MHz intolerance detection.		
	<i>disable</i>	Disable HT 40 MHz intolerance detection.		
ht-greenfield	Enable/disable HT greenfield detection (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HT greenfield detection.</td></tr><tr><td><i>disable</i></td><td>Disable HT greenfield detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable HT greenfield detection.	<i>disable</i>	Disable HT greenfield detection.			
	Option	Description								
	<i>enable</i>	Enable HT greenfield detection.								
<i>disable</i>	Disable HT greenfield detection.									
invalid-addr-combination	Enable/disable invalid address combination detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable invalid address combination detection.</td></tr><tr><td><i>disable</i></td><td>Disable invalid address combination detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable invalid address combination detection.	<i>disable</i>	Disable invalid address combination detection.			
	Option	Description								
	<i>enable</i>	Enable invalid address combination detection.								
<i>disable</i>	Disable invalid address combination detection.									
invalid-mac-oui	Enable/disable invalid MAC OUI detection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable invalid MAC OUI detection.</td></tr><tr><td><i>disable</i></td><td>Disable invalid MAC OUI detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable invalid MAC OUI detection.	<i>disable</i>	Disable invalid MAC OUI detection.			
	Option	Description								
	<i>enable</i>	Enable invalid MAC OUI detection.								
<i>disable</i>	Disable invalid MAC OUI detection.									
long-duration-attack	Enable/disable long duration attack detection based on user configured threshold (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable long duration attack detection.</td></tr><tr><td><i>disable</i></td><td>Disable long duration attack detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable long duration attack detection.	<i>disable</i>	Disable long duration attack detection.			
	Option	Description								
	<i>enable</i>	Enable long duration attack detection.								
<i>disable</i>	Disable long duration attack detection.									
long-duration-thresh	Threshold value for long duration attack detection (1000 - 32767 usec, default = 8200).	integer	Minimum value: 1000 Maximum value: 32767	8200						
malformed-association	Enable/disable malformed association request detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable malformed association request detection.</td></tr><tr><td><i>disable</i></td><td>Disable malformed association request detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable malformed association request detection.	<i>disable</i>	Disable malformed association request detection.			
	Option	Description								
	<i>enable</i>	Enable malformed association request detection.								
<i>disable</i>	Disable malformed association request detection.									
malformed-auth	Enable/disable malformed auth frame detection (default = disable).	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable malformed auth frame detection.		
	<i>disable</i>	Disable malformed auth frame detection.		
malformed-ht-ie	Enable/disable malformed HT IE detection (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Enable malformed HT IE detection.		
	<i>disable</i>	Disable malformed HT IE detection.		
name	WIDS profile name.	string	Maximum length: 35	
netstumbler	Enable/disable netstumbler detection (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Enable netstumbler detection.		
	<i>disable</i>	Disable netstumbler detection.		
netstumbler-thresh	The threshold value for netstumbler.	integer	Minimum value: 1 Maximum value: 65100	5
netstumbler-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	30
null-ssid-probe-resp	Enable/disable null SSID probe response detection (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Enable null SSID probe resp detection.		
	<i>disable</i>	Disable null SSID probe resp detection.		
omerta-attack	Enable/disable omerta attack detection (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable omerta attack detection.		
	<i>disable</i>	Disable omerta attack detection.		
overflow-ie	Enable/disable overflow IE detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable overflow IE detection.		
	<i>disable</i>	Disable overflow IE detection.		
probe-flood	Enable/disable probe flood detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable probe flood detection.		
	<i>disable</i>	Disable probe flood detection.		
probe-flood-thresh	The threshold value for probe flood.	integer	Minimum value: 1 Maximum value: 65100	30
probe-flood-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	1
pspoll-flood	Enable/disable pspoll flood detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable pspoll flood detection.		
	<i>disable</i>	Disable pspoll flood detection.		
pspoll-flood-thresh	The threshold value for pspoll flood.	integer	Minimum value: 1 Maximum value: 65100	30

Parameter	Description	Type	Size	Default						
pspoll-flood-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	1						
pwsave-dos-attack	Enable/disable power save DOS attack detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable power save DOS attack detection.</td></tr><tr><td>disable</td><td>Disable power save DOS attack detection.</td></tr></table>	Option	Description	enable	Enable power save DOS attack detection.	disable	Disable power save DOS attack detection.			
Option	Description									
enable	Enable power save DOS attack detection.									
disable	Disable power save DOS attack detection.									
reassoc-flood	Enable/disable reassociation flood detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reassociation flood detection.</td></tr><tr><td>disable</td><td>Disable reassociation flood detection.</td></tr></table>	Option	Description	enable	Enable reassociation flood detection.	disable	Disable reassociation flood detection.			
Option	Description									
enable	Enable reassociation flood detection.									
disable	Disable reassociation flood detection.									
reassoc-flood-thresh	The threshold value for reassociation flood.	integer	Minimum value: 1 Maximum value: 65100	30						
reassoc-flood-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	10						
risky-encryption	Enable/disable Risky Encryption detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Risky Encryption detection.</td></tr><tr><td>disable</td><td>Disable Risky Encryption detection.</td></tr></table>	Option	Description	enable	Enable Risky Encryption detection.	disable	Disable Risky Encryption detection.			
Option	Description									
enable	Enable Risky Encryption detection.									
disable	Disable Risky Encryption detection.									
rts-flood	Enable/disable rts flood detection (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable rts flood detection.</td></tr><tr><td>disable</td><td>Disable rts flood detection.</td></tr></table>	Option	Description	enable	Enable rts flood detection.	disable	Disable rts flood detection.			
Option	Description									
enable	Enable rts flood detection.									
disable	Disable rts flood detection.									

Parameter	Description	Type	Size	Default
rts-flood-thresh	The threshold value for rts flood.	integer	Minimum value: 1 Maximum value: 65100	30
rts-flood-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	10
sensor-mode	Scan nearby WiFi stations (default = disable).	option	-	disable
	Option Description			
	<i>disable</i>	Disable the scan.		
	<i>foreign</i>	Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.		
	<i>both</i>	Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.		
spoofed-deauth	Enable/disable spoofed de-authentication attack detection (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Enable spoofed de-authentication attack detection.		
	<i>disable</i>	Disable spoofed de-authentication attack detection.		
unencrypted-valid	Enable/disable unencrypted valid detection (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Enable unencrypted valid detection.		
	<i>disable</i>	Disable unencrypted valid detection.		
valid-client-misassociation	Enable/disable valid client misassociation detection (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Enable valid client misassociation detection.		
	<i>disable</i>	Disable valid client misassociation detection.		
valid-ssid-misuse	Enable/disable valid SSID misuse detection (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable valid SSID misuse detection.		
	<i>disable</i>	Disable valid SSID misuse detection.		
weak-wep-iv	Enable/disable weak WEP IV (Initialization Vector) detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable weak WEP IV detection.		
	<i>disable</i>	Disable weak WEP IV detection.		
wellenreiter	Enable/disable wellenreiter detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable wellenreiter detection.		
	<i>disable</i>	Disable wellenreiter detection.		
wellenreiter-thresh	The threshold value for wellenreiter.	integer	Minimum value: 1 Maximum value: 65100	5
wellenreiter-time	Detection Window Period.	integer	Minimum value: 1 Maximum value: 120	30
windows-bridge	Enable/disable windows bridge detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable windows bridge detection.		
	<i>disable</i>	Disable windows bridge detection.		
wireless-bridge	Enable/disable wireless bridge detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable wireless bridge detection.		
	<i>disable</i>	Disable wireless bridge detection.		

Parameter	Description	Type	Size	Default
wpa-ft-attack	Enable/disable WPA FT attack detection (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WPA FT attack detection.		
	<i>disable</i>	Disable WPA FT attack detection.		

config wireless-controller wtp

Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be managed by FortiGate.

```
config wireless-controller wtp
  Description: Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be
  managed by FortiGate.
  edit <wtp-id>
    set admin [discovered|disable|...]
    set allowaccess {option1}, {option2}, ...
    set apcfg-profile {string}
    set ble-major-id {integer}
    set ble-minor-id {integer}
    set bonjour-profile {string}
    set comment {var-string}
    set coordinate-latitude {string}
    set coordinate-longitude {string}
    set firmware-provision {string}
    set firmware-provision-latest [disable|once]
    set image-download [enable|disable]
    set index {integer}
    set ip-fragment-preventing {option1}, {option2}, ...
  config lan
    Description: WTP LAN port mapping.
    set port-esl-mode [offline|nat-to-wan|...]
    set port-esl-ssid {string}
    set port-mode [offline|nat-to-wan|...]
    set port-ssid {string}
    set port1-mode [offline|nat-to-wan|...]
    set port1-ssid {string}
    set port2-mode [offline|nat-to-wan|...]
    set port2-ssid {string}
    set port3-mode [offline|nat-to-wan|...]
    set port3-ssid {string}
    set port4-mode [offline|nat-to-wan|...]
    set port4-ssid {string}
    set port5-mode [offline|nat-to-wan|...]
    set port5-ssid {string}
    set port6-mode [offline|nat-to-wan|...]
    set port6-ssid {string}
```

```

    set port7-mode [offline|nat-to-wan|...]
    set port7-ssid {string}
    set port8-mode [offline|nat-to-wan|...]
    set port8-ssid {string}
end
set led-state [enable|disable]
set location {string}
set login-passwd {password}
set login-passwd-change [yes|default|...]
set mesh-bridge-enable [default|enable|...]
set name {string}
set override-allowaccess [enable|disable]
set override-ip-fragment [enable|disable]
set override-lan [enable|disable]
set override-led-state [enable|disable]
set override-login-passwd-change [enable|disable]
set override-split-tunnel [enable|disable]
set override-wan-port-mode [enable|disable]
set purdue-level [1|1.5|...]
config radio-1
    Description: Configuration options for radio 1.
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set auto-power-target {string}
    set band {option1}, {option2}, ...
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
    set override-band [enable|disable]
    set override-channel [enable|disable]
    set override-txpower [enable|disable]
    set override-vaps [enable|disable]
    set power-level {integer}
    set power-mode [dBm|percentage]
    set power-value {integer}
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
end
config radio-2
    Description: Configuration options for radio 2.
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set auto-power-target {string}
    set band {option1}, {option2}, ...
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
    set override-band [enable|disable]
    set override-channel [enable|disable]
    set override-txpower [enable|disable]
    set override-vaps [enable|disable]
    set power-level {integer}

```

```

    set power-mode [dBm|percentage]
    set power-value {integer}
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
end
config radio-3
    Description: Configuration options for radio 3.
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set auto-power-target {string}
    set band {option1}, {option2}, ...
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
    set override-band [enable|disable]
    set override-channel [enable|disable]
    set override-txpower [enable|disable]
    set override-vaps [enable|disable]
    set power-level {integer}
    set power-mode [dBm|percentage]
    set power-value {integer}
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
end
config radio-4
    Description: Configuration options for radio 4.
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set auto-power-target {string}
    set band {option1}, {option2}, ...
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
    set override-band [enable|disable]
    set override-channel [enable|disable]
    set override-txpower [enable|disable]
    set override-vaps [enable|disable]
    set power-level {integer}
    set power-mode [dBm|percentage]
    set power-value {integer}
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
end
set region {string}
set region-x {string}
set region-y {string}
config split-tunneling-acl
    Description: Split tunneling ACL filter list.
    edit <id>
        set dest-ip {ipv4-classnet}
    next
end

```

```

set split-tunneling-acl-local-ap-subnet [enable|disable]
set split-tunneling-acl-path [tunnel|local]
set tun-mtu-downlink {integer}
set tun-mtu-uplink {integer}
set uuid {uuid}
set wan-port-mode [wan-lan|wan-only]
set wtp-profile {string}
next
end

```

config wireless-controller wtp

Parameter	Description	Type	Size	Default								
admin	Configure how the FortiGate operating as a wireless controller discovers and manages this WTP, AP or FortiAP.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discovered</i></td><td>FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.</td></tr><tr><td><i>disable</i></td><td>FortiGate wireless controller is configured to not provide service to this WTP.</td></tr><tr><td><i>enable</i></td><td>FortiGate wireless controller is configured to provide service to this WTP.</td></tr></table>	Option	Description	<i>discovered</i>	FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.	<i>disable</i>	FortiGate wireless controller is configured to not provide service to this WTP.	<i>enable</i>	FortiGate wireless controller is configured to provide service to this WTP.			
Option	Description											
<i>discovered</i>	FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.											
<i>disable</i>	FortiGate wireless controller is configured to not provide service to this WTP.											
<i>enable</i>	FortiGate wireless controller is configured to provide service to this WTP.											
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr></table>	Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.			
Option	Description											
<i>https</i>	HTTPS access.											
<i>ssh</i>	SSH access.											
<i>snmp</i>	SNMP access.											
apcfg-profile	AP local configuration profile name.	string	Maximum length: 35									
ble-major-id	Override BLE Major ID.	integer	Minimum value: 0 0 Maximum value: 65535									
ble-minor-id	Override BLE Minor ID.	integer	Minimum value: 0 0 Maximum value: 65535									

Parameter	Description	Type	Size	Default						
bonjour-profile	Bonjour profile name.	string	Maximum length: 35							
comment	Comment.	var-string	Maximum length: 255							
coordinate-latitude	WTP latitude coordinate.	string	Maximum length: 19							
coordinate-longitude	WTP longitude coordinate.	string	Maximum length: 19							
firmware-provision	Firmware version to provision to this FortiAP on bootup (major.minor.build, i.e. 6.2.1234).	string	Maximum length: 35							
firmware-provision-latest	Enable/disable one-time automatic provisioning of the latest firmware version.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not automatically provision the latest available firmware.</td></tr><tr><td>once</td><td>Automatically attempt a one-time upgrade to the latest available firmware version.</td></tr></table>				Option	Description	disable	Do not automatically provision the latest available firmware.	once	Automatically attempt a one-time upgrade to the latest available firmware version.
Option	Description									
disable	Do not automatically provision the latest available firmware.									
once	Automatically attempt a one-time upgrade to the latest available firmware version.									
image-download	Enable/disable WTP image download.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WTP image download at join time.</td></tr><tr><td>disable</td><td>Disable WTP image download at join time.</td></tr></table>				Option	Description	enable	Enable WTP image download at join time.	disable	Disable WTP image download at join time.
Option	Description									
enable	Enable WTP image download at join time.									
disable	Disable WTP image download at join time.									
index	Index (0 - 4294967295). Read-only.	integer	Minimum value: 0 0 Maximum value: 4294967295							
ip-fragment-preventing	Method(s) by which IP fragmentation is prevented for control and data packets through CAPWAP tunnel (default = tcp-mss-adjust).	option	-	tcp-mss-adjust						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tcp-mss-adjust</td><td>TCP maximum segment size adjustment.</td></tr><tr><td>icmp-unreachable</td><td>Drop packet and send ICMP Destination Unreachable</td></tr></table>				Option	Description	tcp-mss-adjust	TCP maximum segment size adjustment.	icmp-unreachable	Drop packet and send ICMP Destination Unreachable
Option	Description									
tcp-mss-adjust	TCP maximum segment size adjustment.									
icmp-unreachable	Drop packet and send ICMP Destination Unreachable									

Parameter	Description	Type	Size	Default								
led-state	Enable to allow the FortiAPs LEDs to light. Disable to keep the LEDs off. You may want to keep the LEDs off so they are not distracting in low light areas etc.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow the LEDs on this FortiAP to light.</td></tr><tr><td>disable</td><td>Keep the LEDs on this FortiAP off.</td></tr></table>	Option	Description	enable	Allow the LEDs on this FortiAP to light.	disable	Keep the LEDs on this FortiAP off.					
Option	Description											
enable	Allow the LEDs on this FortiAP to light.											
disable	Keep the LEDs on this FortiAP off.											
location	Field for describing the physical location of the WTP, AP or FortiAP.	string	Maximum length: 35									
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified									
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP (yes, default, or no, default = no).	option	-	no								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>yes</td><td>Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.</td></tr><tr><td>default</td><td>Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.</td></tr><tr><td>no</td><td>Do not change the managed WTP, FortiAP or AP's administrator password.</td></tr></table>	Option	Description	yes	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.	default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.	no	Do not change the managed WTP, FortiAP or AP's administrator password.			
Option	Description											
yes	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.											
default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.											
no	Do not change the managed WTP, FortiAP or AP's administrator password.											
mesh-bridge-enable	Enable/disable mesh Ethernet bridge when WTP is configured as a mesh branch/leaf AP.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Use mesh Ethernet bridge local setting on the WTP.</td></tr><tr><td>enable</td><td>Turn on mesh Ethernet bridge on the WTP.</td></tr><tr><td>disable</td><td>Turn off mesh Ethernet bridge on the WTP.</td></tr></table>	Option	Description	default	Use mesh Ethernet bridge local setting on the WTP.	enable	Turn on mesh Ethernet bridge on the WTP.	disable	Turn off mesh Ethernet bridge on the WTP.			
Option	Description											
default	Use mesh Ethernet bridge local setting on the WTP.											
enable	Turn on mesh Ethernet bridge on the WTP.											
disable	Turn off mesh Ethernet bridge on the WTP.											
name	WTP, AP or FortiAP configuration name.	string	Maximum length: 35									
override-allowaccess	Enable to override the WTP profile management access configuration.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Override the WTP profile management access configuration.		
	<i>disable</i>	Use the WTP profile management access configuration.		
override-ip-fragment	Enable/disable overriding the WTP profile IP fragment prevention setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile IP fragment prevention setting.		
	<i>disable</i>	Use the WTP profile IP fragment prevention setting.		
override-lan	Enable to override the WTP profile LAN port setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile LAN port setting.		
	<i>disable</i>	Use the WTP profile LAN port setting.		
override-led-state	Enable to override the profile LED state setting for this FortiAP. You must enable this option to use the led-state command to turn off the FortiAP's LEDs.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile LED state.		
	<i>disable</i>	Use the WTP profile LED state.		
override-login-passwd-change	Enable to override the WTP profile login-password (administrator password) setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile login-password (administrator password) setting.		
	<i>disable</i>	Use the the WTP profile login-password (administrator password) setting.		
override-split-tunnel	Enable/disable overriding the WTP profile split tunneling setting.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Override the WTP profile split tunneling setting.		
	<i>disable</i>	Use the WTP profile split tunneling setting.		
override-wan-port-mode	Enable/disable overriding the wan-port-mode in the WTP profile.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile wan-port-mode.		
	<i>disable</i>	Use the wan-port-mode in the WTP profile.		
purdue-level	Purdue Level of this WTP.	option	-	3
	Option	Description		
	1	Level 1 - Basic Control		
	1.5	Level 1.5		
	2	Level 2 - Area Supervisory Control		
	2.5	Level 2.5		
	3	Level 3 - Operations & Control		
	3.5	Level 3.5		
	4	Level 4 - Business Planning & Logistics		
	5	Level 5 - Enterprise Network		
5.5	Level 5.5			
region	Region name WTP is associated with.	string	Maximum length: 35	
region-x	Relative horizontal region coordinate (between 0 and 1).	string	Maximum length: 15	0
region-y	Relative vertical region coordinate (between 0 and 1).	string	Maximum length: 15	0
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		
	<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-	local
	Option	Description		
	<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.		
	<i>local</i>	Split tunneling ACL list traffic will be local NATed.		
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel (576 - 1500 bytes or 0; 0 means the local MTU of FortiAP; default = 0).	integer	Minimum value: 576 Maximum value: 1500	0
tun-mtu-uplink	The maximum transmission unit (MTU) of uplink CAPWAP tunnel (576 - 1500 bytes or 0; 0 means the local MTU of FortiAP; default = 0).	integer	Minimum value: 576 Maximum value: 1500	0
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wan-port-mode	Enable/disable using the FortiAP WAN port as a LAN port.	option	-	wan-only
	Option	Description		
	<i>wan-lan</i>	Use the FortiAP WAN port as a LAN port.		
	<i>wan-only</i>	Do not use the WAN port as a LAN port.		
wtp-id	WTP ID.	string	Maximum length: 35	
wtp-profile	WTP profile name to apply to this WTP, AP or FortiAP.	string	Maximum length: 35	

config lan

Parameter	Description	Type	Size	Default
port-esl-mode	ESL port mode.	option	-	offline
	Option	Description		
	offline	Offline.		
	nat-to-wan	NAT WTP ESL port to WTP WAN port.		
	bridge-to-wan	Bridge WTP ESL port to WTP WAN port.		
	bridge-to-ssid	Bridge WTP ESL port to SSID.		
port-esl-ssid	Bridge ESL port to SSID.	string	Maximum length: 15	
port-mode	LAN port mode.	option	-	offline
	Option	Description		
	offline	Offline.		
	nat-to-wan	NAT WTP LAN port to WTP WAN port.		
	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.		
	bridge-to-ssid	Bridge WTP LAN port to SSID.		
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15	
port1-mode	LAN port 1 mode.	option	-	offline
	Option	Description		
	offline	Offline.		
	nat-to-wan	NAT WTP LAN port to WTP WAN port.		
	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.		
	bridge-to-ssid	Bridge WTP LAN port to SSID.		
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15	
port2-mode	LAN port 2 mode.	option	-	offline
	Option	Description		
	offline	Offline.		
	nat-to-wan	NAT WTP LAN port to WTP WAN port.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.							
	Option	Description												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15											
port3-mode	LAN port 3 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
	Option	Description												
	<i>offline</i>	Offline.												
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15											
port4-mode	LAN port 4 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
	Option	Description												
	<i>offline</i>	Offline.												
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15											
port5-mode	LAN port 5 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
	Option	Description												
	<i>offline</i>	Offline.												
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15											
port6-mode	LAN port 6 mode.	option	-	offline										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15	
port7-mode	LAN port 7 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15	
port8-mode	LAN port 8 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15	

config radio-1

Parameter	Description	Type	Size	Default
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17

Parameter	Description	Type	Size	Default																												
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-	disable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable automatic transmit power adjustment.</td></tr><tr><td>disable</td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	enable	Enable automatic transmit power adjustment.	disable	Disable automatic transmit power adjustment.																									
	Option	Description																														
	enable	Enable automatic transmit power adjustment.																														
disable	Disable automatic transmit power adjustment.																															
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 10 0 Maximum value: 4294967295																													
auto-power-target	Target of automatic transmit power adjustment in dBm (-95 to -20, default = -70).	string	Maximum length: 7	-70																												
band	WiFi band that Radio 1 operates on.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g.</td></tr><tr><td>802.11n-2G</td><td>802.11n (WiFi 4) at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n (WiFi 4) at 5GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac (WiFi 5) at 2.4GHz.</td></tr><tr><td>802.11ac-5G</td><td>802.11ac (WiFi 5) at 5GHz.</td></tr><tr><td>802.11ax-2G</td><td>802.11ax (WiFi 6) at 2.4GHz.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax (WiFi 6) at 5GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax (WiFi 6) at 6GHz.</td></tr><tr><td>802.11be-2G</td><td>802.11be (WiFi 7) at 2.4GHz.</td></tr><tr><td>802.11be-5G</td><td>802.11be (WiFi 7) at 5GHz.</td></tr><tr><td>802.11be-6G</td><td>802.11be (WiFi 7) at 6GHz.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g.	802.11n-2G	802.11n (WiFi 4) at 2.4GHz.	802.11n-5G	802.11n (WiFi 4) at 5GHz.	802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.	802.11ac-5G	802.11ac (WiFi 5) at 5GHz.	802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.	802.11ax-5G	802.11ax (WiFi 6) at 5GHz.	802.11ax-6G	802.11ax (WiFi 6) at 6GHz.	802.11be-2G	802.11be (WiFi 7) at 2.4GHz.	802.11be-5G	802.11be (WiFi 7) at 5GHz.	802.11be-6G	802.11be (WiFi 7) at 6GHz.			
	Option	Description																														
	802.11a	802.11a.																														
	802.11b	802.11b.																														
	802.11g	802.11g.																														
	802.11n-2G	802.11n (WiFi 4) at 2.4GHz.																														
	802.11n-5G	802.11n (WiFi 4) at 5GHz.																														
	802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.																														
	802.11ac-5G	802.11ac (WiFi 5) at 5GHz.																														
	802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.																														
	802.11ax-5G	802.11ax (WiFi 6) at 5GHz.																														
	802.11ax-6G	802.11ax (WiFi 6) at 6GHz.																														
	802.11be-2G	802.11be (WiFi 7) at 2.4GHz.																														
802.11be-5G	802.11be (WiFi 7) at 5GHz.																															
802.11be-6G	802.11be (WiFi 7) at 6GHz.																															
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3																													
drma-manual-mode	Radio mode to be used for DRMA manual mode (default = ncf).	option	-	ncf																												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ap</i>	Set the radio to AP mode.		
	<i>monitor</i>	Set the radio to monitor mode		
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		
override-band	Enable to override the WTP profile band setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
override-tpower	Enable to override the WTP profile power level configuration.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile power level configuration.		
	<i>disable</i>	Use the WTP profile power level configuration.		
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100	100

Parameter	Description	Type	Size	Default								
power-mode	Set radio effective isotropic radiated power (EIRP) in dBm or by a percentage of the maximum EIRP (default = percentage). This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.					
Option	Description											
<i>dBm</i>	Set radio EIRP power in dBm.											
<i>percentage</i>	Set radio EIRP power by percentage.											
power-value	Radio EIRP power in dBm (1 - 33, default = 27).	integer	Minimum value: 1 Maximum value: 33	27								
vap-all	Configure method for assigning SSIDs to this FortiAP (default = automatically assign tunnel SSIDs).	option	-	tunnel								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									

config radio-2

Parameter	Description	Type	Size	Default				
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17				
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-	disable				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr></table>				Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.
Option	Description							
<i>enable</i>	Enable automatic transmit power adjustment.							

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	Target of automatic transmit power adjustment in dBm (-95 to -20, default = -70).	string	Maximum length: 7	-70
band	WiFi band that Radio 2 operates on.	option	-	
	Option	Description		
	<i>802.11a</i>	802.11a.		
	<i>802.11b</i>	802.11b.		
	<i>802.11g</i>	802.11g.		
	<i>802.11n-2G</i>	802.11n (WiFi 4) at 2.4GHz.		
	<i>802.11n-5G</i>	802.11n (WiFi 4) at 5GHz.		
	<i>802.11ac-2G</i>	802.11ac (WiFi 5) at 2.4GHz.		
	<i>802.11ac-5G</i>	802.11ac (WiFi 5) at 5GHz.		
	<i>802.11ax-2G</i>	802.11ax (WiFi 6) at 2.4GHz.		
	<i>802.11ax-5G</i>	802.11ax (WiFi 6) at 5GHz.		
	<i>802.11ax-6G</i>	802.11ax (WiFi 6) at 6GHz.		
	<i>802.11be-2G</i>	802.11be (WiFi 7) at 2.4GHz.		
	<i>802.11be-5G</i>	802.11be (WiFi 7) at 5GHz.		
	<i>802.11be-6G</i>	802.11be (WiFi 7) at 6GHz.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
drma-manual-mode	Radio mode to be used for DRMA manual mode (default = ncf).	option	-	ncf
	Option	Description		
	<i>ap</i>	Set the radio to AP mode.		
	<i>monitor</i>	Set the radio to monitor mode		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		
override-band	Enable to override the WTP profile band setting.	option	-	disable
	Option Description			
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	Option Description			
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable
	Option Description			
	<i>enable</i>	Override the WTP profile power level configuration.		
	<i>disable</i>	Use the WTP profile power level configuration.		
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	Option Description			
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100	100

Parameter	Description	Type	Size	Default								
power-mode	Set radio effective isotropic radiated power (EIRP) in dBm or by a percentage of the maximum EIRP (default = percentage). This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.					
Option	Description											
<i>dBm</i>	Set radio EIRP power in dBm.											
<i>percentage</i>	Set radio EIRP power by percentage.											
power-value	Radio EIRP power in dBm (1 - 33, default = 27).	integer	Minimum value: 1 Maximum value: 33	27								
vap-all	Configure method for assigning SSIDs to this FortiAP (default = automatically assign tunnel SSIDs).	option	-	tunnel								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									

config radio-3

Parameter	Description	Type	Size	Default				
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17				
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-	disable				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr></table>				Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.
Option	Description							
<i>enable</i>	Enable automatic transmit power adjustment.							

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>disable</i>	Disable automatic transmit power adjustment.																											
Option	Description																															
<i>disable</i>	Disable automatic transmit power adjustment.																															
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10																												
auto-power-target	Target of automatic transmit power adjustment in dBm (-95 to -20, default = -70).	string	Maximum length: 7	-70																												
band	WiFi band that Radio 3 operates on.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.11a</i></td><td>802.11a.</td></tr><tr><td><i>802.11b</i></td><td>802.11b.</td></tr><tr><td><i>802.11g</i></td><td>802.11g.</td></tr><tr><td><i>802.11n-2G</i></td><td>802.11n (WiFi 4) at 2.4GHz.</td></tr><tr><td><i>802.11n-5G</i></td><td>802.11n (WiFi 4) at 5GHz.</td></tr><tr><td><i>802.11ac-2G</i></td><td>802.11ac (WiFi 5) at 2.4GHz.</td></tr><tr><td><i>802.11ac-5G</i></td><td>802.11ac (WiFi 5) at 5GHz.</td></tr><tr><td><i>802.11ax-2G</i></td><td>802.11ax (WiFi 6) at 2.4GHz.</td></tr><tr><td><i>802.11ax-5G</i></td><td>802.11ax (WiFi 6) at 5GHz.</td></tr><tr><td><i>802.11ax-6G</i></td><td>802.11ax (WiFi 6) at 6GHz.</td></tr><tr><td><i>802.11be-2G</i></td><td>802.11be (WiFi 7) at 2.4GHz.</td></tr><tr><td><i>802.11be-5G</i></td><td>802.11be (WiFi 7) at 5GHz.</td></tr><tr><td><i>802.11be-6G</i></td><td>802.11be (WiFi 7) at 6GHz.</td></tr></table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g.	<i>802.11n-2G</i>	802.11n (WiFi 4) at 2.4GHz.	<i>802.11n-5G</i>	802.11n (WiFi 4) at 5GHz.	<i>802.11ac-2G</i>	802.11ac (WiFi 5) at 2.4GHz.	<i>802.11ac-5G</i>	802.11ac (WiFi 5) at 5GHz.	<i>802.11ax-2G</i>	802.11ax (WiFi 6) at 2.4GHz.	<i>802.11ax-5G</i>	802.11ax (WiFi 6) at 5GHz.	<i>802.11ax-6G</i>	802.11ax (WiFi 6) at 6GHz.	<i>802.11be-2G</i>	802.11be (WiFi 7) at 2.4GHz.	<i>802.11be-5G</i>	802.11be (WiFi 7) at 5GHz.	<i>802.11be-6G</i>	802.11be (WiFi 7) at 6GHz.			
Option	Description																															
<i>802.11a</i>	802.11a.																															
<i>802.11b</i>	802.11b.																															
<i>802.11g</i>	802.11g.																															
<i>802.11n-2G</i>	802.11n (WiFi 4) at 2.4GHz.																															
<i>802.11n-5G</i>	802.11n (WiFi 4) at 5GHz.																															
<i>802.11ac-2G</i>	802.11ac (WiFi 5) at 2.4GHz.																															
<i>802.11ac-5G</i>	802.11ac (WiFi 5) at 5GHz.																															
<i>802.11ax-2G</i>	802.11ax (WiFi 6) at 2.4GHz.																															
<i>802.11ax-5G</i>	802.11ax (WiFi 6) at 5GHz.																															
<i>802.11ax-6G</i>	802.11ax (WiFi 6) at 6GHz.																															
<i>802.11be-2G</i>	802.11be (WiFi 7) at 2.4GHz.																															
<i>802.11be-5G</i>	802.11be (WiFi 7) at 5GHz.																															
<i>802.11be-6G</i>	802.11be (WiFi 7) at 6GHz.																															
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3																													
drma-manual-mode	Radio mode to be used for DRMA manual mode (default = ncf).	option	-	ncf																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ap</i></td><td>Set the radio to AP mode.</td></tr><tr><td><i>monitor</i></td><td>Set the radio to monitor mode</td></tr></table>	Option	Description	<i>ap</i>	Set the radio to AP mode.	<i>monitor</i>	Set the radio to monitor mode																									
Option	Description																															
<i>ap</i>	Set the radio to AP mode.																															
<i>monitor</i>	Set the radio to monitor mode																															

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ncf</i></td><td>Select and set the radio mode based on NCF score.</td></tr><tr><td><i>ncf-peek</i></td><td>Select the radio mode based on NCF score, but do not apply.</td></tr></table>				Option	Description	<i>ncf</i>	Select and set the radio mode based on NCF score.	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.
	Option	Description								
	<i>ncf</i>	Select and set the radio mode based on NCF score.								
<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.									
override-band	Enable to override the WTP profile band setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the WTP profile band setting.</td></tr><tr><td><i>disable</i></td><td>Use the WTP profile band setting.</td></tr></table>				Option	Description	<i>enable</i>	Override the WTP profile band setting.	<i>disable</i>	Use the WTP profile band setting.
	Option	Description								
	<i>enable</i>	Override the WTP profile band setting.								
<i>disable</i>	Use the WTP profile band setting.									
override-channel	Enable to override WTP profile channel settings.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override WTP profile channel settings.</td></tr><tr><td><i>disable</i></td><td>Use WTP profile channel settings.</td></tr></table>				Option	Description	<i>enable</i>	Override WTP profile channel settings.	<i>disable</i>	Use WTP profile channel settings.
	Option	Description								
	<i>enable</i>	Override WTP profile channel settings.								
<i>disable</i>	Use WTP profile channel settings.									
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the WTP profile power level configuration.</td></tr><tr><td><i>disable</i></td><td>Use the WTP profile power level configuration.</td></tr></table>				Option	Description	<i>enable</i>	Override the WTP profile power level configuration.	<i>disable</i>	Use the WTP profile power level configuration.
	Option	Description								
	<i>enable</i>	Override the WTP profile power level configuration.								
<i>disable</i>	Use the WTP profile power level configuration.									
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override WTP profile VAP settings.</td></tr><tr><td><i>disable</i></td><td>Use WTP profile VAP settings.</td></tr></table>				Option	Description	<i>enable</i>	Override WTP profile VAP settings.	<i>disable</i>	Use WTP profile VAP settings.
	Option	Description								
	<i>enable</i>	Override WTP profile VAP settings.								
<i>disable</i>	Use WTP profile VAP settings.									
power-level	Radio EIRP power level as a percentage of the maximum EIRP power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100	100						

Parameter	Description	Type	Size	Default								
power-mode	Set radio effective isotropic radiated power (EIRP) in dBm or by a percentage of the maximum EIRP (default = percentage). This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.					
Option	Description											
<i>dBm</i>	Set radio EIRP power in dBm.											
<i>percentage</i>	Set radio EIRP power by percentage.											
power-value	Radio EIRP power in dBm (1 - 33, default = 27).	integer	Minimum value: 1 Maximum value: 33	27								
vap-all	Configure method for assigning SSIDs to this FortiAP (default = automatically assign tunnel SSIDs).	option	-	tunnel								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									

config radio-4

Parameter	Description	Type	Size	Default				
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17				
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-	disable				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr></table>				Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.
Option	Description							
<i>enable</i>	Enable automatic transmit power adjustment.							

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>disable</i>	Disable automatic transmit power adjustment.																											
Option	Description																															
<i>disable</i>	Disable automatic transmit power adjustment.																															
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10																												
auto-power-target	Target of automatic transmit power adjustment in dBm (-95 to -20, default = -70).	string	Maximum length: 7	-70																												
band	WiFi band that Radio 4 operates on.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.11a</i></td><td>802.11a.</td></tr><tr><td><i>802.11b</i></td><td>802.11b.</td></tr><tr><td><i>802.11g</i></td><td>802.11g.</td></tr><tr><td><i>802.11n-2G</i></td><td>802.11n (WiFi 4) at 2.4GHz.</td></tr><tr><td><i>802.11n-5G</i></td><td>802.11n (WiFi 4) at 5GHz.</td></tr><tr><td><i>802.11ac-2G</i></td><td>802.11ac (WiFi 5) at 2.4GHz.</td></tr><tr><td><i>802.11ac-5G</i></td><td>802.11ac (WiFi 5) at 5GHz.</td></tr><tr><td><i>802.11ax-2G</i></td><td>802.11ax (WiFi 6) at 2.4GHz.</td></tr><tr><td><i>802.11ax-5G</i></td><td>802.11ax (WiFi 6) at 5GHz.</td></tr><tr><td><i>802.11ax-6G</i></td><td>802.11ax (WiFi 6) at 6GHz.</td></tr><tr><td><i>802.11be-2G</i></td><td>802.11be (WiFi 7) at 2.4GHz.</td></tr><tr><td><i>802.11be-5G</i></td><td>802.11be (WiFi 7) at 5GHz.</td></tr><tr><td><i>802.11be-6G</i></td><td>802.11be (WiFi 7) at 6GHz.</td></tr></table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g.	<i>802.11n-2G</i>	802.11n (WiFi 4) at 2.4GHz.	<i>802.11n-5G</i>	802.11n (WiFi 4) at 5GHz.	<i>802.11ac-2G</i>	802.11ac (WiFi 5) at 2.4GHz.	<i>802.11ac-5G</i>	802.11ac (WiFi 5) at 5GHz.	<i>802.11ax-2G</i>	802.11ax (WiFi 6) at 2.4GHz.	<i>802.11ax-5G</i>	802.11ax (WiFi 6) at 5GHz.	<i>802.11ax-6G</i>	802.11ax (WiFi 6) at 6GHz.	<i>802.11be-2G</i>	802.11be (WiFi 7) at 2.4GHz.	<i>802.11be-5G</i>	802.11be (WiFi 7) at 5GHz.	<i>802.11be-6G</i>	802.11be (WiFi 7) at 6GHz.			
Option	Description																															
<i>802.11a</i>	802.11a.																															
<i>802.11b</i>	802.11b.																															
<i>802.11g</i>	802.11g.																															
<i>802.11n-2G</i>	802.11n (WiFi 4) at 2.4GHz.																															
<i>802.11n-5G</i>	802.11n (WiFi 4) at 5GHz.																															
<i>802.11ac-2G</i>	802.11ac (WiFi 5) at 2.4GHz.																															
<i>802.11ac-5G</i>	802.11ac (WiFi 5) at 5GHz.																															
<i>802.11ax-2G</i>	802.11ax (WiFi 6) at 2.4GHz.																															
<i>802.11ax-5G</i>	802.11ax (WiFi 6) at 5GHz.																															
<i>802.11ax-6G</i>	802.11ax (WiFi 6) at 6GHz.																															
<i>802.11be-2G</i>	802.11be (WiFi 7) at 2.4GHz.																															
<i>802.11be-5G</i>	802.11be (WiFi 7) at 5GHz.																															
<i>802.11be-6G</i>	802.11be (WiFi 7) at 6GHz.																															
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3																													
drma-manual-mode	Radio mode to be used for DRMA manual mode (default = ncf).	option	-	ncf																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ap</i></td><td>Set the radio to AP mode.</td></tr><tr><td><i>monitor</i></td><td>Set the radio to monitor mode</td></tr></table>	Option	Description	<i>ap</i>	Set the radio to AP mode.	<i>monitor</i>	Set the radio to monitor mode																									
Option	Description																															
<i>ap</i>	Set the radio to AP mode.																															
<i>monitor</i>	Set the radio to monitor mode																															

Parameter	Description	Type	Size	Default
	Option Description			
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		
override-band	Enable to override the WTP profile band setting.	option	-	disable
	Option Description			
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	Option Description			
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable
	Option Description			
	<i>enable</i>	Override the WTP profile power level configuration.		
	<i>disable</i>	Use the WTP profile power level configuration.		
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	Option Description			
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100	100

Parameter	Description	Type	Size	Default								
power-mode	Set radio effective isotropic radiated power (EIRP) in dBm or by a percentage of the maximum EIRP (default = percentage). This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.					
Option	Description											
<i>dBm</i>	Set radio EIRP power in dBm.											
<i>percentage</i>	Set radio EIRP power by percentage.											
power-value	Radio EIRP power in dBm (1 - 33, default = 27).	integer	Minimum value: 1 Maximum value: 33	27								
vap-all	Configure method for assigning SSIDs to this FortiAP (default = automatically assign tunnel SSIDs).	option	-	tunnel								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									

config split-tunneling-acl

Parameter	Description	Type	Size	Default
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config wireless-controller wtp-group

Configure WTP groups.

```

config wireless-controller wtp-group
  Description: Configure WTP groups.
  edit <name>
    set ble-major-id {integer}
    set platform-type [AP-11N|C24JE|...]
    set wtps <wtp-id1>, <wtp-id2>, ...
  next
end

```

config wireless-controller wtp-group

Parameter	Description	Type	Size	Default
ble-major-id	Override BLE Major ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	WTP group name.	string	Maximum length: 35	
platform-type	FortiAP models to define the WTP group platform type.	option	-	

Option	Description
<i>AP-11N</i>	Default 11n AP.
<i>C24JE</i>	FAPC24JE.
<i>421E</i>	FAP421E.
<i>423E</i>	FAP423E.
<i>221E</i>	FAP221E.
<i>222E</i>	FAP222E.
<i>223E</i>	FAP223E.
<i>224E</i>	FAP224E.
<i>231E</i>	FAP231E.
<i>321E</i>	FAP321E.
<i>431F</i>	FAP431F.
<i>431FL</i>	FAP431FL.
<i>432F</i>	FAP432F.
<i>432FR</i>	FAP432FR.
<i>433F</i>	FAP433F.

Parameter	Description	Type	Size	Default
	Option	Description		
	433FL	FAP433FL.		
	231F	FAP231F.		
	231FL	FAP231FL.		
	234F	FAP234F.		
	23JF	FAP23JF.		
	831F	FAP831F.		
	231G	FAP231G.		
	233G	FAP233G.		
	234G	FAP234G.		
	431G	FAP431G.		
	432G	FAP432G.		
	433G	FAP433G.		
	231K	FAP231K.		
	23JK	FAP23JK.		
	241K	FAP241K.		
	243K	FAP243K.		
	441K	FAP441K.		
	443K	FAP443K.		
	U421E	FAPU421EV.		
	U422EV	FAPU422EV.		
	U423E	FAPU423EV.		
	U221EV	FAPU221EV.		
	U223EV	FAPU223EV.		
	U24JEV	FAPU24JEV.		
	U321EV	FAPU321EV.		
	U323EV	FAPU323EV.		
	U431F	FAPU431F.		
	U433F	FAPU433F.		
	U231F	FAPU231F.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>U234F</i>	FAPU234F.		
	<i>U432F</i>	FAPU432F.		
	<i>U231G</i>	FAPU231G.		
wtps <wtp-id>	WTP list. WTP ID.	string	Maximum length: 35	

config wireless-controller wtp-profile

Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms.

```
config wireless-controller wtp-profile
    Description: Configure WTP profiles or FortiAP profiles that define radio settings for
manageable FortiAP platforms.
    edit <name>
        set admin-auth-tacacs+ {string}
        set admin-restrict-local [enable|disable]
        set allowaccess {option1}, {option2}, ...
        set ap-country [--|AF|...]
        set ap-handoff [enable|disable]
        set apcfg-profile {string}
        set ble-profile {string}
        set bonjour-profile {string}
        set comment {var-string}
        set console-login [enable|disable]
        set control-message-offload {option1}, {option2}, ...
        config deny-mac-list
            Description: List of MAC addresses that are denied access to this WTP, FortiAP, or AP.
            edit <id>
                set mac {mac-address}
            next
        end
        set dtls-in-kernel [enable|disable]
        set dtls-policy {option1}, {option2}, ...
        set energy-efficient-ethernet [enable|disable]
        config esl-ses-dongle
            Description: ESL SES-imagotag dongle configuration.
            set apc-addr-type [fqdn|ip]
            set apc-fqdn {string}
            set apc-ip {ipv4-address}
            set apc-port {integer}
            set coex-level {option}
            set compliance-level {option}
            set esl-channel [-1|0|...]
            set output-power [a|b|...]
```

```

    set scd-enable [enable|disable]
    set tls-cert-verification [enable|disable]
    set tls-fqdn-verification [enable|disable]
end
set ext-info-enable [enable|disable]
set frequency-handoff [enable|disable]
set handoff-roaming [enable|disable]
set handoff-rssi {integer}
set handoff-sta-thresh {integer}
set indoor-outdoor-deployment [platform-determined|outdoor|...]
set ip-fragment-preventing {option1}, {option2}, ...
config lan
    Description: WTP LAN port mapping.
    set port-esl-mode [offline|nat-to-wan|...]
    set port-esl-ssid {string}
    set port-mode [offline|nat-to-wan|...]
    set port-ssid {string}
    set port1-mode [offline|nat-to-wan|...]
    set port1-ssid {string}
    set port2-mode [offline|nat-to-wan|...]
    set port2-ssid {string}
    set port3-mode [offline|nat-to-wan|...]
    set port3-ssid {string}
    set port4-mode [offline|nat-to-wan|...]
    set port4-ssid {string}
    set port5-mode [offline|nat-to-wan|...]
    set port5-ssid {string}
    set port6-mode [offline|nat-to-wan|...]
    set port6-ssid {string}
    set port7-mode [offline|nat-to-wan|...]
    set port7-ssid {string}
    set port8-mode [offline|nat-to-wan|...]
    set port8-ssid {string}
end
config lbs
    Description: Set various location based service (LBS) options.
    set aeroscout [enable|disable]
    set aeroscout-ap-mac [bssid|board-mac]
    set aeroscout-mmu-report [enable|disable]
    set aeroscout-mu [enable|disable]
    set aeroscout-mu-factor {integer}
    set aeroscout-mu-timeout {integer}
    set aeroscout-server-ip {ipv4-address-any}
    set aeroscout-server-port {integer}
    set ble-rtls [none|polestar|...]
    set ble-rtls-accumulation-interval {integer}
    set ble-rtls-asset-addrgrp-list {string}
    set ble-rtls-asset-uuid-list1 {string}
    set ble-rtls-asset-uuid-list2 {string}
    set ble-rtls-asset-uuid-list3 {string}
    set ble-rtls-asset-uuid-list4 {string}
    set ble-rtls-protocol {option}

```

```

set ble-rtls-reporting-interval {integer}
set ble-rtls-server-fqdn {string}
set ble-rtls-server-path {string}
set ble-rtls-server-port {integer}
set ble-rtls-server-token {string}
set ekahau-blink-mode [enable|disable]
set ekahau-tag {mac-address}
set erc-server-ip {ipv4-address-any}
set erc-server-port {integer}
set fortipresence [foreign|both|...]
set fortipresence-ble [enable|disable]
set fortipresence-frequency {integer}
set fortipresence-port {integer}
set fortipresence-project {string}
set fortipresence-rogue [enable|disable]
set fortipresence-secret {password}
set fortipresence-server {ipv4-address-any}
set fortipresence-server-addr-type [ipv4|fqdn]
set fortipresence-server-fqdn {string}
set fortipresence-unassoc [enable|disable]
set station-locate [enable|disable]
end
set led-schedules <name1>, <name2>, ...
set led-state [enable|disable]
set lldp [enable|disable]
set login-passwd {password}
set login-passwd-change [yes|default|...]
set max-clients {integer}
config platform
    Description: WTP, FortiAP, or AP platform.
    set ddscan [enable|disable]
    set mode [single-5G|dual-5G]
    set type [AP-11N|C24JE|...]
end
set poe-mode [auto|8023af|...]
config radio-1
    Description: Configuration options for radio 1.
    set 80211d [enable|disable]
    set 80211mc [enable|disable]
    set airtime-fairness [enable|disable]
    set amsdu [enable|disable]
    set ap-sniffer-addr {mac-address}
    set ap-sniffer-bufsize {integer}
    set ap-sniffer-chan {integer}
    set ap-sniffer-chan-width [320MHz|240MHz|...]
    set ap-sniffer-ctl [enable|disable]
    set ap-sniffer-data [enable|disable]
    set ap-sniffer-mgmt-beacon [enable|disable]
    set ap-sniffer-mgmt-other [enable|disable]
    set ap-sniffer-mgmt-probe [enable|disable]
    set arrp-profile {string}
    set auto-power-high {integer}

```



```
set auto-power-level [enable|disable]
set auto-power-low {integer}
set auto-power-target {string}
set band {option1}, {option2}, ...
set band-5g-type [5g-full|5g-high|...]
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
set beacon-interval {integer}
set bss-color {integer}
set bss-color-mode [auto|static]
set call-admission-control [enable|disable]
set call-capacity {integer}
set channel <chan1>, <chan2>, ...
set channel-bonding [320MHz|240MHz|...]
set channel-bonding-ext [320MHz-1|320MHz-2]
set channel-utilization [enable|disable]
set coexistence [enable|disable]
set darrp [enable|disable]
set drma [disable|enable]
set drma-sensitivity [low|medium|...]
set dtim {integer}
set frag-threshold {integer}
set iperf-protocol [udp|tcp]
set iperf-server-port {integer}
set max-clients {integer}
set max-distance {integer}
set mimo-mode [default|1x1|...]
set mode [disabled|ap|...]
set optional-antenna [none|custom|...]
set optional-antenna-gain {string}
set power-level {integer}
set power-mode [dBm|percentage]
set power-value {integer}
set powersave-optimize {option1}, {option2}, ...
set protection-mode [rtscts|ctsonly|...]
set rts-threshold {integer}
set sam-bssid {mac-address}
set sam-ca-certificate {string}
set sam-captive-portal [enable|disable]
set sam-client-certificate {string}
set sam-cwp-failure-string {string}
set sam-cwp-match-string {string}
set sam-cwp-password {password}
set sam-cwp-success-string {string}
set sam-cwp-test-url {string}
set sam-cwp-username {string}
set sam-eap-method [both|tls|...]
set sam-password {password}
set sam-private-key {string}
set sam-private-key-password {password}
set sam-report-intv {integer}
set sam-security-type [open|wpa-personal|...]
```

```

set sam-server-fqdn {string}
set sam-server-ip {ipv4-address}
set sam-server-type [ip|fqdn]
set sam-ssid {string}
set sam-test [ping|iperf]
set sam-username {string}
set short-guard-interval [enable|disable]
set transmit-optimize {option1}, {option2}, ...
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set wids-profile {string}
set zero-wait-dfs [enable|disable]
end
config radio-2
    Description: Configuration options for radio 2.
    set 80211d [enable|disable]
    set 80211mc [enable|disable]
    set airtime-fairness [enable|disable]
    set amsdu [enable|disable]
    set ap-sniffer-addr {mac-address}
    set ap-sniffer-bufsize {integer}
    set ap-sniffer-chan {integer}
    set ap-sniffer-chan-width [320MHz|240MHz|...]
    set ap-sniffer-ctl [enable|disable]
    set ap-sniffer-data [enable|disable]
    set ap-sniffer-mgmt-beacon [enable|disable]
    set ap-sniffer-mgmt-other [enable|disable]
    set ap-sniffer-mgmt-probe [enable|disable]
    set arnp-profile {string}
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set auto-power-target {string}
    set band {option1}, {option2}, ...
    set band-5g-type [5g-full|5g-high|...]
    set bandwidth-admission-control [enable|disable]
    set bandwidth-capacity {integer}
    set beacon-interval {integer}
    set bss-color {integer}
    set bss-color-mode [auto|static]
    set call-admission-control [enable|disable]
    set call-capacity {integer}
    set channel <chan1>, <chan2>, ...
    set channel-bonding [320MHz|240MHz|...]
    set channel-bonding-ext [320MHz-1|320MHz-2]
    set channel-utilization [enable|disable]
    set coexistence [enable|disable]
    set darrp [enable|disable]
    set drma [disable|enable]
    set drma-sensitivity [low|medium|...]
    set dtim {integer}
    set frag-threshold {integer}

```

```

set iperf-protocol [udp|tcp]
set iperf-server-port {integer}
set max-clients {integer}
set max-distance {integer}
set mimo-mode [default|1x1|...]
set mode [disabled|ap|...]
set optional-antenna [none|custom|...]
set optional-antenna-gain {string}
set power-level {integer}
set power-mode [dBm|percentage]
set power-value {integer}
set powersave-optimize {option1}, {option2}, ...
set protection-mode [rtscts|ctsonly|...]
set rts-threshold {integer}
set sam-bssid {mac-address}
set sam-ca-certificate {string}
set sam-captive-portal [enable|disable]
set sam-client-certificate {string}
set sam-cwp-failure-string {string}
set sam-cwp-match-string {string}
set sam-cwp-password {password}
set sam-cwp-success-string {string}
set sam-cwp-test-url {string}
set sam-cwp-username {string}
set sam-eap-method [both|tls|...]
set sam-password {password}
set sam-private-key {string}
set sam-private-key-password {password}
set sam-report-intv {integer}
set sam-security-type [open|wpa-personal|...]
set sam-server-fqdn {string}
set sam-server-ip {ipv4-address}
set sam-server-type [ip|fqdn]
set sam-ssid {string}
set sam-test [ping|iperf]
set sam-username {string}
set short-guard-interval [enable|disable]
set transmit-optimize {option1}, {option2}, ...
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set wids-profile {string}
set zero-wait-dfs [enable|disable]
end
config radio-3
  Description: Configuration options for radio 3.
  set 80211d [enable|disable]
  set 80211mc [enable|disable]
  set airtime-fairness [enable|disable]
  set amsdu [enable|disable]
  set ap-sniffer-addr {mac-address}
  set ap-sniffer-bufsize {integer}
  set ap-sniffer-chan {integer}

```

```
set ap-sniffer-chan-width [320MHz|240MHz|...]
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set arrp-profile {string}
set auto-power-high {integer}
set auto-power-level [enable|disable]
set auto-power-low {integer}
set auto-power-target {string}
set band {option1}, {option2}, ...
set band-5g-type [5g-full|5g-high|...]
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
set beacon-interval {integer}
set bss-color {integer}
set bss-color-mode [auto|static]
set call-admission-control [enable|disable]
set call-capacity {integer}
set channel <chan1>, <chan2>, ...
set channel-bonding [320MHz|240MHz|...]
set channel-bonding-ext [320MHz-1|320MHz-2]
set channel-utilization [enable|disable]
set coexistence [enable|disable]
set darrp [enable|disable]
set drma [disable|enable]
set drma-sensitivity [low|medium|...]
set dtim {integer}
set frag-threshold {integer}
set iperf-protocol [udp|tcp]
set iperf-server-port {integer}
set max-clients {integer}
set max-distance {integer}
set mimo-mode [default|1x1|...]
set mode [disabled|ap|...]
set optional-antenna [none|custom|...]
set optional-antenna-gain {string}
set power-level {integer}
set power-mode [dBm|percentage]
set power-value {integer}
set powersave-optimize {option1}, {option2}, ...
set protection-mode [rtscts|ctsonly|...]
set rts-threshold {integer}
set sam-bssid {mac-address}
set sam-ca-certificate {string}
set sam-captive-portal [enable|disable]
set sam-client-certificate {string}
set sam-cwp-failure-string {string}
set sam-cwp-match-string {string}
set sam-cwp-password {password}
set sam-cwp-success-string {string}
```

```

set sam-cwp-test-url {string}
set sam-cwp-username {string}
set sam-eap-method [both|tls|...]
set sam-password {password}
set sam-private-key {string}
set sam-private-key-password {password}
set sam-report-intv {integer}
set sam-security-type [open|wpa-personal|...]
set sam-server-fqdn {string}
set sam-server-ip {ipv4-address}
set sam-server-type [ip|fqdn]
set sam-ssid {string}
set sam-test [ping|iperf]
set sam-username {string}
set short-guard-interval [enable|disable]
set transmit-optimize {option1}, {option2}, ...
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set wids-profile {string}
set zero-wait-dfs [enable|disable]
end
config radio-4
    Description: Configuration options for radio 4.
    set 80211d [enable|disable]
    set 80211mc [enable|disable]
    set airtime-fairness [enable|disable]
    set amsdu [enable|disable]
    set ap-sniffer-addr {mac-address}
    set ap-sniffer-bufsize {integer}
    set ap-sniffer-chan {integer}
    set ap-sniffer-chan-width [320MHz|240MHz|...]
    set ap-sniffer-ctl [enable|disable]
    set ap-sniffer-data [enable|disable]
    set ap-sniffer-mgmt-beacon [enable|disable]
    set ap-sniffer-mgmt-other [enable|disable]
    set ap-sniffer-mgmt-probe [enable|disable]
    set arrp-profile {string}
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set auto-power-target {string}
    set band {option1}, {option2}, ...
    set band-5g-type [5g-full|5g-high|...]
    set bandwidth-admission-control [enable|disable]
    set bandwidth-capacity {integer}
    set beacon-interval {integer}
    set bss-color {integer}
    set bss-color-mode [auto|static]
    set call-admission-control [enable|disable]
    set call-capacity {integer}
    set channel <chan1>, <chan2>, ...
    set channel-bonding [320MHz|240MHz|...]

```

```

set channel-bonding-ext [320MHz-1|320MHz-2]
set channel-utilization [enable|disable]
set coexistence [enable|disable]
set darrp [enable|disable]
set drma [disable|enable]
set drma-sensitivity [low|medium|...]
set dtim {integer}
set frag-threshold {integer}
set iperf-protocol [udp|tcp]
set iperf-server-port {integer}
set max-clients {integer}
set max-distance {integer}
set mimo-mode [default|1x1|...]
set mode [disabled|ap|...]
set optional-antenna [none|custom|...]
set optional-antenna-gain {string}
set power-level {integer}
set power-mode [dBm|percentage]
set power-value {integer}
set powersave-optimize {option1}, {option2}, ...
set protection-mode [rtscts|ctsonly|...]
set rts-threshold {integer}
set sam-bssid {mac-address}
set sam-ca-certificate {string}
set sam-captive-portal [enable|disable]
set sam-client-certificate {string}
set sam-cwp-failure-string {string}
set sam-cwp-match-string {string}
set sam-cwp-password {password}
set sam-cwp-success-string {string}
set sam-cwp-test-url {string}
set sam-cwp-username {string}
set sam-eap-method [both|tls|...]
set sam-password {password}
set sam-private-key {string}
set sam-private-key-password {password}
set sam-report-intv {integer}
set sam-security-type [open|wpa-personal|...]
set sam-server-fqdn {string}
set sam-server-ip {ipv4-address}
set sam-server-type [ip|fqdn]
set sam-ssid {string}
set sam-test [ping|iperf]
set sam-username {string}
set short-guard-interval [enable|disable]
set transmit-optimize {option1}, {option2}, ...
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set wids-profile {string}
set zero-wait-dfs [enable|disable]
end
config split-tunneling-acl

```

```

Description: Split tunneling ACL filter list.
edit <id>
    set dest-ip {ipv4-classnet}
next
end
set split-tunneling-acl-local-ap-subnet [enable|disable]
set split-tunneling-acl-path [tunnel|local]
set syslog-profile {string}
set tun-mtu-downlink {integer}
set tun-mtu-uplink {integer}
set unii-4-5ghz-band [enable|disable]
set usb-port [enable|disable]
set wan-port-auth [none|802.1x]
set wan-port-auth-macsec [enable|disable]
set wan-port-auth-methods [all|EAP-FAST|...]
set wan-port-auth-password {password}
set wan-port-auth-username {string}
set wan-port-mode [wan-lan|wan-only]
next
end

```

config wireless-controller wtp-profile

Parameter	Description	Type	Size	Default								
admin-auth-tacacs+	Remote authentication server for admin user.	string	Maximum length: 35									
admin-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local admin authentication restriction.</td></tr><tr><td><i>disable</i></td><td>Diable local admin authentication restriction.</td></tr></table>				Option	Description	<i>enable</i>	Enable local admin authentication restriction.	<i>disable</i>	Diable local admin authentication restriction.		
Option	Description											
<i>enable</i>	Enable local admin authentication restriction.											
<i>disable</i>	Diable local admin authentication restriction.											
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr></table>				Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.
Option	Description											
<i>https</i>	HTTPS access.											
<i>ssh</i>	SSH access.											
<i>snmp</i>	SNMP access.											

Parameter	Description	Type	Size	Default
ap-country	Country in which this WTP, FortiAP, or AP will operate (default = NA, automatically use the country configured for the current VDOM).	option	-	--

Option	Description
--	NO_COUNTRY_SET
AF	AFGHANISTAN
AL	ALBANIA
DZ	ALGERIA
AS	AMERICAN SAMOA
AO	ANGOLA
AR	ARGENTINA
AM	ARMENIA
AU	AUSTRALIA
AT	AUSTRIA
AZ	AZERBAIJAN
BS	BAHAMAS
BH	BAHRAIN
BD	BANGLADESH
BB	BARBADOS
BY	BELARUS
BE	BELGIUM
BZ	BELIZE
BJ	BENIN
BM	BERMUDA
BT	BHUTAN
BO	BOLIVIA
BA	BOSNIA AND HERZEGOVINA
BW	BOTSWANA
BR	BRAZIL
BN	BRUNEI DARUSSALAM

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>BG</i>	BULGARIA		
	<i>BF</i>	BURKINA-FASO		
	<i>KH</i>	CAMBODIA		
	<i>CM</i>	CAMEROON		
	<i>KY</i>	CAYMAN ISLANDS		
	<i>CF</i>	CENTRAL AFRICA REPUBLIC		
	<i>TD</i>	CHAD		
	<i>CL</i>	CHILE		
	<i>CN</i>	CHINA		
	<i>CX</i>	CHRISTMAS ISLAND		
	<i>CO</i>	COLOMBIA		
	<i>CG</i>	CONGO REPUBLIC		
	<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO		
	<i>CR</i>	COSTA RICA		
	<i>HR</i>	CROATIA		
	<i>CY</i>	CYPRUS		
	<i>CZ</i>	CZECH REPUBLIC		
	<i>DK</i>	DENMARK		
	<i>DJ</i>	DJIBOUTI		
	<i>DM</i>	DOMINICA		
	<i>DO</i>	DOMINICAN REPUBLIC		
	<i>EC</i>	ECUADOR		
	<i>EG</i>	EGYPT		
	<i>SV</i>	EL SALVADOR		
	<i>ET</i>	ETHIOPIA		
	<i>EE</i>	ESTONIA		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		
	<i>FO</i>	FAEROE ISLANDS		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GA</i>	GABON		
	<i>GE</i>	GEORGIA		
	<i>GM</i>	GAMBIA		
	<i>DE</i>	GERMANY		
	<i>GH</i>	GHANA		
	<i>GI</i>	GIBRALTAR		
	<i>GR</i>	GREECE		
	<i>GL</i>	GREENLAND		
	<i>GD</i>	GRENADA		
	<i>GP</i>	GUADELOUPE		
	<i>GU</i>	GUAM		
	<i>GT</i>	GUATEMALA		
	<i>GY</i>	GUYANA		
	<i>HT</i>	HAITI		
	<i>HN</i>	HONDURAS		
	<i>HK</i>	HONG KONG		
	<i>HU</i>	HUNGARY		
	<i>IS</i>	ICELAND		
	<i>IN</i>	INDIA		
	<i>ID</i>	INDONESIA		
	<i>IQ</i>	IRAQ		
	<i>IE</i>	IRELAND		
	<i>IM</i>	ISLE OF MAN		
	<i>IL</i>	ISRAEL		
	<i>IT</i>	ITALY		
	<i>CI</i>	COTE_D_IVOIRE		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>JM</i>	JAMAICA		
	<i>JO</i>	JORDAN		
	<i>KZ</i>	KAZAKHSTAN		
	<i>KE</i>	KENYA		
	<i>KR</i>	KOREA REPUBLIC		
	<i>KW</i>	KUWAIT		
	<i>LA</i>	LAOS		
	<i>LV</i>	LATVIA		
	<i>LB</i>	LEBANON		
	<i>LS</i>	LESOTHO		
	<i>LR</i>	LIBERIA		
	<i>LY</i>	LIBYA		
	<i>LI</i>	LIECHTENSTEIN		
	<i>LT</i>	LITHUANIA		
	<i>LU</i>	LUXEMBOURG		
	<i>MO</i>	MACAU SAR		
	<i>MK</i>	MACEDONIA, FYRO		
	<i>MG</i>	MADAGASCAR		
	<i>MW</i>	MALAWI		
	<i>MY</i>	MALAYSIA		
	<i>MV</i>	MALDIVES		
	<i>ML</i>	MALI		
	<i>MT</i>	MALTA		
	<i>MH</i>	MARSHALL ISLANDS		
	<i>MQ</i>	MARTINIQUE		
	<i>MR</i>	MAURITANIA		
	<i>MU</i>	MAURITIUS		
	<i>YT</i>	MAYOTTE		
	<i>MX</i>	MEXICO		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>FM</i>	MICRONESIA		
	<i>MD</i>	REPUBLIC OF MOLDOVA		
	<i>MC</i>	MONACO		
	<i>MN</i>	MONGOLIA		
	<i>MA</i>	MOROCCO		
	<i>MZ</i>	MOZAMBIQUE		
	<i>MM</i>	MYANMAR		
	<i>NA</i>	NAMIBIA		
	<i>NP</i>	NEPAL		
	<i>NL</i>	NETHERLANDS		
	<i>AN</i>	NETHERLANDS ANTILLES		
	<i>AW</i>	ARUBA		
	<i>NZ</i>	NEW ZEALAND		
	<i>NI</i>	NICARAGUA		
	<i>NE</i>	NIGER		
	<i>NG</i>	NIGERIA		
	<i>NO</i>	NORWAY		
	<i>MP</i>	NORTHERN MARIANA ISLANDS		
	<i>OM</i>	OMAN		
	<i>PK</i>	PAKISTAN		
	<i>PW</i>	PALAU		
	<i>PA</i>	PANAMA		
	<i>PG</i>	PAPUA NEW GUINEA		
	<i>PY</i>	PARAGUAY		
	<i>PE</i>	PERU		
	<i>PH</i>	PHILIPPINES		
	<i>PL</i>	POLAND		
	<i>PT</i>	PORTUGAL		
	<i>PR</i>	PUERTO RICO		

Parameter	Description	Type	Size	Default
	Option	Description		
	QA	QATAR		
	RE	REUNION		
	RO	ROMANIA		
	RU	RUSSIA		
	RW	RWANDA		
	BL	SAINT BARTHELEMY		
	KN	SAINT KITTS AND NEVIS		
	LC	SAINT LUCIA		
	MF	SAINT MARTIN		
	PM	SAINT PIERRE AND MIQUELON		
	VC	SAINT VINCENT AND GRENADIENS		
	SA	SAUDI ARABIA		
	SN	SENEGAL		
	RS	REPUBLIC OF SERBIA		
	ME	MONTENEGRO		
	SL	SIERRA LEONE		
	SG	SINGAPORE		
	SK	SLOVAKIA		
	SI	SLOVENIA		
	SO	SOMALIA		
	ZA	SOUTH AFRICA		
	ES	SPAIN		
	LK	SRI LANKA		
	SR	SURINAME		
	SZ	SWAZILAND		
	SE	SWEDEN		
	CH	SWITZERLAND		
	TW	TAIWAN		
	TZ	TANZANIA		

Parameter	Description	Type	Size	Default
	Option	Description		
	TH	THAILAND		
	TL	TIMOR-LESTE		
	TG	TOGO		
	TT	TRINIDAD AND TOBAGO		
	TN	TUNISIA		
	TR	TURKEY		
	TM	TURKMENISTAN		
	AE	UNITED ARAB EMIRATES		
	TC	TURKS AND CAICOS		
	UG	UGANDA		
	UA	UKRAINE		
	GB	UNITED KINGDOM		
	US	UNITED STATES2		
	PS	UNITED STATES (PUBLIC SAFETY)		
	UY	URUGUAY		
	UZ	UZBEKISTAN		
	VU	VANUATU		
	VE	VENEZUELA		
	VN	VIET NAM		
	VI	VIRGIN ISLANDS		
	WF	WALLIS AND FUTUNA		
	YE	YEMEN		
	ZM	ZAMBIA		
	ZW	ZIMBABWE		
	JP	JAPAN14		
	CA	CANADA2		
ap-handoff	Enable/disable AP handoff of clients to other APs (default = disable).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable AP handoff.		
	<i>disable</i>	Disable AP handoff.		
apcfg-profile	AP local configuration profile name.	string	Maximum length: 35	
ble-profile	Bluetooth Low Energy profile name.	string	Maximum length: 35	
bonjour-profile	Bonjour profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
console-login	Enable/disable FortiAP console login access (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FAP console login access.		
	<i>disable</i>	Disable FAP console login access.		
control-message-offload	Enable/disable CAPWAP control message data channel offload.	option	-	ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health spectral-analysis
	Option	Description		
	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.		
	<i>aeroscout-tag</i>	AeroScout tag.		
	<i>ap-list</i>	Rogue AP list.		
	<i>sta-list</i>	Rogue STA list.		
	<i>sta-cap-list</i>	STA capability list.		
	<i>stats</i>	WTP, radio, VAP, and STA statistics.		
	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.		
	<i>sta-health</i>	STA health log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>spectral-analysis</i>	Spectral analysis report.		
dtls-in-kernel	Enable/disable data channel DTLS in kernel.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable data channel DTLS in kernel.		
	<i>disable</i>	Disable data channel DTLS in kernel.		
dtls-policy	WTP data channel DTLS policy (default = clear-text).	option	-	clear-text
	Option	Description		
	<i>clear-text</i>	Clear Text Data Channel.		
	<i>dtls-enabled</i>	DTLS Enabled Data Channel.		
	<i>ipsec-vpn</i>	IPsec VPN Data Channel.		
	<i>ipsec-sn-vpn</i>	IPsec VPN Data Channel with FortiAP's SN in the first IKE messages.		
energy-efficient-ethernet	Enable/disable use of energy efficient Ethernet on WTP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of energy efficient Ethernet on WTP.		
	<i>disable</i>	Disable use of energy efficient Ethernet on WTP.		
ext-info-enable	Enable/disable station/VAP/radio extension information.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable station/VAP/radio extension information.		
	<i>disable</i>	Disable station/VAP/radio extension information.		
frequency-handoff	Enable/disable frequency handoff of clients to other channels (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable frequency handoff.		
	<i>disable</i>	Disable frequency handoff.		

Parameter	Description	Type	Size	Default								
handoff-roaming	Enable/disable client load balancing during roaming to avoid roaming delay (default = disable).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable handoff roaming.</td></tr><tr><td><i>disable</i></td><td>Disable handoff roaming.</td></tr></table>	Option	Description	<i>enable</i>	Enable handoff roaming.	<i>disable</i>	Disable handoff roaming.					
Option	Description											
<i>enable</i>	Enable handoff roaming.											
<i>disable</i>	Disable handoff roaming.											
handoff-rssi	Minimum received signal strength indicator (RSSI) value for handoff (20 - 30, default = 25).	integer	Minimum value: 20 Maximum value: 30	25								
handoff-sta-thresh	Threshold value for AP handoff.	integer	Minimum value: 5 Maximum value: 60	0								
indoor-outdoor-deployment	Set to allow indoor/outdoor-only channels under regulatory rules (default = platform-determined).	option	-	platform-determined								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>platform-determined</i></td><td>Set AP deployment type based on its platform.</td></tr><tr><td><i>outdoor</i></td><td>Set AP deployment type to outdoor.</td></tr><tr><td><i>indoor</i></td><td>Set AP deployment type to indoor.</td></tr></table>	Option	Description	<i>platform-determined</i>	Set AP deployment type based on its platform.	<i>outdoor</i>	Set AP deployment type to outdoor.	<i>indoor</i>	Set AP deployment type to indoor.			
Option	Description											
<i>platform-determined</i>	Set AP deployment type based on its platform.											
<i>outdoor</i>	Set AP deployment type to outdoor.											
<i>indoor</i>	Set AP deployment type to indoor.											
ip-fragment-preventing	Method(s) by which IP fragmentation is prevented for control and data packets through CAPWAP tunnel (default = tcp-mss-adjust).	option	-	tcp-mss-adjust								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp-mss-adjust</i></td><td>TCP maximum segment size adjustment.</td></tr><tr><td><i>icmp-unreachable</i></td><td>Drop packet and send ICMP Destination Unreachable</td></tr></table>	Option	Description	<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.	<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable					
Option	Description											
<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.											
<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable											
led-schedules <name>	Recurring firewall schedules for illuminating LEDs on the FortiAP. If led-state is enabled, LEDs will be visible when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default								
led-state	Enable/disable use of LEDs on WTP (default = disable).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of LEDs on WTP.</td></tr><tr><td>disable</td><td>Disable use of LEDs on WTP.</td></tr></table>	Option	Description	enable	Enable use of LEDs on WTP.	disable	Disable use of LEDs on WTP.					
Option	Description											
enable	Enable use of LEDs on WTP.											
disable	Disable use of LEDs on WTP.											
lldp	Enable/disable Link Layer Discovery Protocol (LLDP) for the WTP, FortiAP, or AP (default = enable).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable LLDP.</td></tr><tr><td>disable</td><td>Disable LLDP.</td></tr></table>	Option	Description	enable	Enable LLDP.	disable	Disable LLDP.					
Option	Description											
enable	Enable LLDP.											
disable	Disable LLDP.											
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified									
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP (yes, default, or no, default = no).	option	-	no								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>yes</td><td>Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.</td></tr><tr><td>default</td><td>Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.</td></tr><tr><td>no</td><td>Do not change the managed WTP, FortiAP or AP's administrator password.</td></tr></table>	Option	Description	yes	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.	default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.	no	Do not change the managed WTP, FortiAP or AP's administrator password.			
Option	Description											
yes	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.											
default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.											
no	Do not change the managed WTP, FortiAP or AP's administrator password.											
max-clients	Maximum number of stations (STAs) supported by the WTP (default = 0, meaning no client limitation).	integer	Minimum value: 0 Maximum value: 4294967295									
name	WTP (or FortiAP or AP) profile name.	string	Maximum length: 35									
poe-mode	Set the WTP, FortiAP, or AP's PoE mode.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Automatically detect the PoE mode.</td></tr><tr><td>8023af</td><td>Use 802.3af PoE mode.</td></tr></table>	Option	Description	auto	Automatically detect the PoE mode.	8023af	Use 802.3af PoE mode.					
Option	Description											
auto	Automatically detect the PoE mode.											
8023af	Use 802.3af PoE mode.											

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>8023at</td><td>Use 802.3at PoE mode.</td></tr><tr><td>power-adapter</td><td>Use the power adapter to control the PoE mode.</td></tr><tr><td>full</td><td>Use full power mode.</td></tr><tr><td>high</td><td>Use high power mode.</td></tr><tr><td>low</td><td>Use low power mode.</td></tr></table>	Option	Description	8023at	Use 802.3at PoE mode.	power-adapter	Use the power adapter to control the PoE mode.	full	Use full power mode.	high	Use high power mode.	low	Use low power mode.			
	Option	Description														
	8023at	Use 802.3at PoE mode.														
	power-adapter	Use the power adapter to control the PoE mode.														
	full	Use full power mode.														
	high	Use high power mode.														
low	Use low power mode.															
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL (default = disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.</td></tr><tr><td>disable</td><td>Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.</td></tr></table>	Option	Description	enable	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.	disable	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.									
	Option	Description														
	enable	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.														
disable	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.															
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-	local												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tunnel</td><td>Split tunneling ACL list traffic will be tunnel.</td></tr><tr><td>local</td><td>Split tunneling ACL list traffic will be local NATed.</td></tr></table>	Option	Description	tunnel	Split tunneling ACL list traffic will be tunnel.	local	Split tunneling ACL list traffic will be local NATed.									
	Option	Description														
	tunnel	Split tunneling ACL list traffic will be tunnel.														
local	Split tunneling ACL list traffic will be local NATed.															
syslog-profile	System log server configuration profile name.	string	Maximum length: 35													
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel (576 - 1500 bytes or 0; 0 means the local MTU of FortiAP; default = 0).	integer	Minimum value: 0 576 Maximum value: 1500													
tun-mtu-uplink	The maximum transmission unit (MTU) of uplink CAPWAP tunnel (576 - 1500 bytes or 0; 0 means the local MTU of FortiAP; default = 0).	integer	Minimum value: 0 576 Maximum value: 1500													
unii-4-5ghz-band	Enable/disable UNII-4 5Ghz band channels (default = disable).	option	-	disable												

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable UNII-4 5Ghz band channels.		
	<i>disable</i>	Disable UNII-4 5Ghz band channels.		
usb-port	Enable/disable USB port of the WTP (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable USB port.		
	<i>disable</i>	Disable USB port.		
wan-port-auth	Set WAN port authentication mode (default = none).	option	-	none
	Option Description			
	<i>none</i>	Disable WAN port authentication.		
	<i>802.1x</i>	Enable WAN port 802.1x authentication.		
wan-port-auth-macsec	Enable/disable WAN port 802.1x supplicant MACsec policy (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Enable WAN port 802.1x supplicant MACsec policy.		
	<i>disable</i>	Disable WAN port 802.1x supplicant MACsec policy.		
wan-port-auth-methods	WAN port 802.1x supplicant EAP methods (default = all).	option	-	all
	Option Description			
	<i>all</i>	Do not specify any EAP methods.		
	<i>EAP-FAST</i>	Enable EAP-FAST.		
	<i>EAP-TLS</i>	Enable EAP-TLS.		
	<i>EAP-PEAP</i>	Enable EAP-PEAP.		
wan-port-auth-password	Set WAN port 802.1x supplicant password.	password	Not Specified	
wan-port-auth-username	Set WAN port 802.1x supplicant user name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
wan-port-mode	Enable/disable using a WAN port as a LAN port.	option	-	wan-only						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wan-lan</td><td>Enable using a WAN port as a LAN port.</td></tr><tr><td>wan-only</td><td>Disable using a WAN port as a LAN port.</td></tr></table>				Option	Description	wan-lan	Enable using a WAN port as a LAN port.	wan-only	Disable using a WAN port as a LAN port.
Option	Description									
wan-lan	Enable using a WAN port as a LAN port.									
wan-only	Disable using a WAN port as a LAN port.									

config deny-mac-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
mac	A WiFi device with this MAC address is denied access to this WTP, FortiAP or AP.	mac-address	Not Specified	00:00:00:00:00:00

config esl-ses-dongle

Parameter	Description	Type	Size	Default
apc-addr-type	ESL SES-imagotag APC address type (default = fqdn).	option	-	fqdn
	Option	Description		
	fqdn	Fully Qualified Domain Name address.		
	ip	IPv4 address.		
apc-fqdn	FQDN of ESL SES-imagotag Access Point Controller (APC).	string	Maximum length: 63	
apc-ip	IP address of ESL SES-imagotag Access Point Controller (APC).	ipv4-address	Not Specified	0.0.0.0
apc-port	Port of ESL SES-imagotag Access Point Controller (APC).	integer	Minimum value: 0 Maximum value: 65535	0
coex-level	ESL SES-imagotag dongle coexistence level (default = none).	option	-	none

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No support for coexistence of USB-Dongle with WiFi AP.</td></tr></table>	Option	Description	<i>none</i>	No support for coexistence of USB-Dongle with WiFi AP.																											
Option	Description																															
<i>none</i>	No support for coexistence of USB-Dongle with WiFi AP.																															
compliance-level	Compliance levels for the ESL solution integration (default = compliance-level-2).	option	-	compliance-level-2																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>compliance-level-2</i></td><td>Compliance Level 2 - Full Cloud Support, IoT and Fast-Response.</td></tr></table>	Option	Description	<i>compliance-level-2</i>	Compliance Level 2 - Full Cloud Support, IoT and Fast-Response.																											
Option	Description																															
<i>compliance-level-2</i>	Compliance Level 2 - Full Cloud Support, IoT and Fast-Response.																															
esl-channel	ESL SES-imagotag dongle channel (default = 127).	option	-	127																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>-1</i></td><td>No esl-channel is set.</td></tr><tr><td><i>0</i></td><td>ESL channel 0.</td></tr><tr><td><i>1</i></td><td>ESL channel 1.</td></tr><tr><td><i>2</i></td><td>ESL channel 2.</td></tr><tr><td><i>3</i></td><td>ESL channel 3.</td></tr><tr><td><i>4</i></td><td>ESL channel 4.</td></tr><tr><td><i>5</i></td><td>ESL channel 5.</td></tr><tr><td><i>6</i></td><td>ESL channel 6.</td></tr><tr><td><i>7</i></td><td>ESL channel 7.</td></tr><tr><td><i>8</i></td><td>ESL channel 8.</td></tr><tr><td><i>9</i></td><td>ESL channel 9.</td></tr><tr><td><i>10</i></td><td>ESL channel 10.</td></tr><tr><td><i>127</i></td><td>Managed channel enabled, indicates that the APC (server) is setting the esl-channel via the slot channel</td></tr></table>	Option	Description	<i>-1</i>	No esl-channel is set.	<i>0</i>	ESL channel 0.	<i>1</i>	ESL channel 1.	<i>2</i>	ESL channel 2.	<i>3</i>	ESL channel 3.	<i>4</i>	ESL channel 4.	<i>5</i>	ESL channel 5.	<i>6</i>	ESL channel 6.	<i>7</i>	ESL channel 7.	<i>8</i>	ESL channel 8.	<i>9</i>	ESL channel 9.	<i>10</i>	ESL channel 10.	<i>127</i>	Managed channel enabled, indicates that the APC (server) is setting the esl-channel via the slot channel			
Option	Description																															
<i>-1</i>	No esl-channel is set.																															
<i>0</i>	ESL channel 0.																															
<i>1</i>	ESL channel 1.																															
<i>2</i>	ESL channel 2.																															
<i>3</i>	ESL channel 3.																															
<i>4</i>	ESL channel 4.																															
<i>5</i>	ESL channel 5.																															
<i>6</i>	ESL channel 6.																															
<i>7</i>	ESL channel 7.																															
<i>8</i>	ESL channel 8.																															
<i>9</i>	ESL channel 9.																															
<i>10</i>	ESL channel 10.																															
<i>127</i>	Managed channel enabled, indicates that the APC (server) is setting the esl-channel via the slot channel																															
output-power	ESL SES-imagotag dongle output power (default = A).	option	-	a																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>a</i></td><td>About 15mW.</td></tr><tr><td><i>b</i></td><td>About 7mW.</td></tr><tr><td><i>c</i></td><td>About 5mW.</td></tr></table>	Option	Description	<i>a</i>	About 15mW.	<i>b</i>	About 7mW.	<i>c</i>	About 5mW.																							
Option	Description																															
<i>a</i>	About 15mW.																															
<i>b</i>	About 7mW.																															
<i>c</i>	About 5mW.																															

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>d</i></td><td>About 1mW.</td></tr><tr><td><i>e</i></td><td>About 13mW.</td></tr><tr><td><i>f</i></td><td>About 10mW.</td></tr><tr><td><i>g</i></td><td>About 3mW.</td></tr><tr><td><i>h</i></td><td>About 2mW.</td></tr></table>	Option	Description	<i>d</i>	About 1mW.	<i>e</i>	About 13mW.	<i>f</i>	About 10mW.	<i>g</i>	About 3mW.	<i>h</i>	About 2mW.			
	Option	Description														
	<i>d</i>	About 1mW.														
	<i>e</i>	About 13mW.														
	<i>f</i>	About 10mW.														
	<i>g</i>	About 3mW.														
<i>h</i>	About 2mW.															
scd-enable	Enable/disable ESL SES-imagotag Serial Communication Daemon (SCD) (default = disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ESL SES-imagotag SCD.</td></tr><tr><td><i>disable</i></td><td>Disable ESL SES-imagotag SCD.</td></tr></table>	Option	Description	<i>enable</i>	Enable ESL SES-imagotag SCD.	<i>disable</i>	Disable ESL SES-imagotag SCD.									
	Option	Description														
	<i>enable</i>	Enable ESL SES-imagotag SCD.														
<i>disable</i>	Disable ESL SES-imagotag SCD.															
tls-cert-verification	Enable/disable TLS certificate verification (default = enable).	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TLS Certificate verification.</td></tr><tr><td><i>disable</i></td><td>Disable TLS Certificate verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable TLS Certificate verification.	<i>disable</i>	Disable TLS Certificate verification.									
	Option	Description														
	<i>enable</i>	Enable TLS Certificate verification.														
<i>disable</i>	Disable TLS Certificate verification.															
tls-fqdn-verification	Enable/disable TLS FQDN verification (default = disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TLS FQDN verification.</td></tr><tr><td><i>disable</i></td><td>Disable TLS FQDN verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable TLS FQDN verification.	<i>disable</i>	Disable TLS FQDN verification.									
	Option	Description														
	<i>enable</i>	Enable TLS FQDN verification.														
<i>disable</i>	Disable TLS FQDN verification.															

config lan

Parameter	Description	Type	Size	Default						
port-esl-mode	ESL port mode.	option	-	offline						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>offline</td><td>Offline.</td></tr><tr><td>nat-to-wan</td><td>NAT WTP ESL port to WTP WAN port.</td></tr></table>				Option	Description	offline	Offline.	nat-to-wan	NAT WTP ESL port to WTP WAN port.
Option	Description									
offline	Offline.									
nat-to-wan	NAT WTP ESL port to WTP WAN port.									

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP ESL port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP ESL port to SSID.</td></tr></table>	Option	Description	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.							
	Option	Description												
	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.													
port-esl-ssid	Bridge ESL port to SSID.	string	Maximum length: 15											
port-mode	LAN port mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
	Option	Description												
	<i>offline</i>	Offline.												
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15											
port1-mode	LAN port 1 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
	Option	Description												
	<i>offline</i>	Offline.												
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15											
port2-mode	LAN port 2 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
	Option	Description												
	<i>offline</i>	Offline.												
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15											
port3-mode	LAN port 3 mode.	option	-	offline										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15	
port4-mode	LAN port 4 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15	
port5-mode	LAN port 5 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15	
port6-mode	LAN port 6 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		

Parameter	Description	Type	Size	Default
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15	
port7-mode	LAN port 7 mode.	option	-	offline
	Option	Description		
	offline	Offline.		
	nat-to-wan	NAT WTP LAN port to WTP WAN port.		
	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.		
	bridge-to-ssid	Bridge WTP LAN port to SSID.		
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15	
port8-mode	LAN port 8 mode.	option	-	offline
	Option	Description		
	offline	Offline.		
	nat-to-wan	NAT WTP LAN port to WTP WAN port.		
	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.		
	bridge-to-ssid	Bridge WTP LAN port to SSID.		
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15	

config lbs

Parameter	Description	Type	Size	Default						
aeroscout	Enable/disable AeroScout Real Time Location Service (RTLS) support (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AeroScout support.</td></tr><tr><td><i>disable</i></td><td>Disable AeroScout support.</td></tr></table>	Option	Description	<i>enable</i>	Enable AeroScout support.	<i>disable</i>	Disable AeroScout support.			
Option	Description									
<i>enable</i>	Enable AeroScout support.									
<i>disable</i>	Disable AeroScout support.									
aeroscout-ap-mac	Use BSSID or board MAC address as AP MAC address in AeroScout AP messages (default = bssid).	option	-	bssid						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>bssid</i>	Use BSSID as AP MAC address in AeroScout AP messages.		
	<i>board-mac</i>	Use board MAC address as AP MAC address in AeroScout AP messages.		
aeroscout-mmureport	Enable/disable compounded AeroScout tag and MU report (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable compounded AeroScout tag and MU report.		
	<i>disable</i>	Disable compounded AeroScout tag and MU report.		
aeroscout-mu	Enable/disable AeroScout Mobile Unit (MU) support (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable AeroScout MU mode support.		
	<i>disable</i>	Disable AeroScout MU mode support.		
aeroscout-mu-factor	AeroScout MU mode dilution factor (default = 20).	integer	Minimum value: 20 0 Maximum value: 4294967295	
aeroscout-mu-timeout	AeroScout MU mode timeout (0 - 65535 sec, default = 5).	integer	Minimum value: 5 0 Maximum value: 65535	
aeroscout-server-ip	IP address of AeroScout server.	ipv4-address-any	Not Specified	0.0.0.0
aeroscout-server-port	AeroScout server UDP listening port.	integer	Minimum value: 0 1024 Maximum value: 65535	
ble-rtls	Set BLE Real Time Location Service (RTLS) support (default = none).	option	-	none
	Option	Description		
	<i>none</i>	Set BLE RTLS to none (default = none).		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>polestar</i>	Set BLE RTLS to PoleStar.		
	<i>evresys</i>	Set BLE RTLS to Evresys.		
ble-rtls-accumulation-interval	Time that measurements should be accumulated in seconds (default = 2).	integer	Minimum value: 2 1 Maximum value: 60	
ble-rtls-asset-addrgrp-list	Tags and asset addrgrp list to be reported.	string	Maximum length: 79	
ble-rtls-asset-uuid-list1	Tags and asset UUID list 1 to be reported (string in the format of 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX').	string	Maximum length: 36	
ble-rtls-asset-uuid-list2	Tags and asset UUID list 2 to be reported (string in the format of 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX').	string	Maximum length: 36	
ble-rtls-asset-uuid-list3	Tags and asset UUID list 3 to be reported (string in the format of 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX').	string	Maximum length: 36	
ble-rtls-asset-uuid-list4	Tags and asset UUID list 4 to be reported (string in the format of 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX').	string	Maximum length: 36	
ble-rtls-protocol	Select the protocol to report Measurements, Advertising Data, or Location Data to Cloud Server (default = WSS).	option	-	WSS
	Option	Description		
	WSS	Use WebSocket protocol to report Measurements, Advertising Data, or Location Data to Cloud Server.		
ble-rtls-reporting-interval	Time between reporting accumulated measurements in seconds (default = 2).	integer	Minimum value: 2 1 Maximum value: 600	
ble-rtls-server-fqdn	FQDN of BLE Real Time Location Service (RTLS) Server.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default
ble-rtls-server-path	Path of BLE Real Time Location Service (RTLS) Server.	string	Maximum length: 255	
ble-rtls-server-port	Port of BLE Real Time Location Service (RTLS) Server (default = 443).	integer	Minimum value: 1 Maximum value: 65535	443
ble-rtls-server-token	Access Token of BLE Real Time Location Service (RTLS) Server.	string	Maximum length: 31	
ekahau-blink-mode	Enable/disable Ekahau blink mode (now known as AiRISTA Flow) to track and locate WiFi tags (default = disable).	option	-	disable
	Option		Description	
	<i>enable</i>		Enable Ekahau blink mode.	
	<i>disable</i>		Disable Ekahau blink mode.	
ekahau-tag	WiFi frame MAC address or WiFi Tag.	mac-address	Not Specified	01:18:8e:00:00:00
erc-server-ip	IP address of Ekahau RTLS Controller (ERC).	ipv4-address-any	Not Specified	0.0.0.0
erc-server-port	Ekahau RTLS Controller (ERC) UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535	8569
fortipresence	Enable/disable FortiPresence to monitor the location and activity of WiFi clients even if they don't connect to this WiFi network (default = disable).	option	-	disable
	Option		Description	
	<i>foreign</i>		FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.	
	<i>both</i>		Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.	
	<i>disable</i>		Disable FortiPresence.	
fortipresence-ble	Enable/disable FortiPresence finding and reporting BLE devices.	option	-	enable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable FortiPresence finding and reporting BLE devices.		
	<i>disable</i>	Disable FortiPresence finding and reporting BLE devices.		
fortipresence-frequency	FortiPresence report transmit frequency (5 - 65535 sec, default = 30).	integer	Minimum value: 30 5 Maximum value: 65535	
fortipresence-port	UDP listening port of FortiPresence server (default = 3000).	integer	Minimum value: 3000 300 Maximum value: 65535	
fortipresence-project	FortiPresence project name (max. 16 characters, default = fortipresence).	string	Maximum length: 16	fortipresence
fortipresence-rogue	Enable/disable FortiPresence finding and reporting rogue APs.	option	-	disable
	Option Description			
	<i>enable</i>	Enable FortiPresence finding and reporting rogue APs.		
	<i>disable</i>	Disable FortiPresence finding and reporting rogue APs.		
fortipresence-secret	FortiPresence secret password (max. 16 characters).	password	Not Specified	
fortipresence-server	IP address of FortiPresence server.	ipv4-address-any	Not Specified	0.0.0.0
fortipresence-server-addr-type	FortiPresence server address type (default = ipv4).	option	-	ipv4
	Option Description			
	<i>ipv4</i>	IPv4 address.		
	<i>fqdn</i>	Fully Qualified Domain Name address.		
fortipresence-server-fqdn	FQDN of FortiPresence server.	string	Maximum length: 255	
fortipresence-unassoc	Enable/disable FortiPresence finding and reporting unassociated stations.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable FortiPresence finding and reporting unassociated stations.		
	<i>disable</i>	Disable FortiPresence finding and reporting unassociated stations.		
station-locate	Enable/disable client station locating services for all clients, whether associated or not (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable station locating service.		
	<i>disable</i>	Disable station locating service.		

config platform

Parameter	Description	Type	Size	Default
ddscan	Enable/disable use of one radio for dedicated full-band scanning to detect RF characterization and wireless threat management.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dedicated full-band scan mode.		
	<i>disable</i>	Disable dedicated full-band scan mode.		
mode	Configure operation mode of 5G radios (default = single-5G).	option	-	single-5G
	Option	Description		
	<i>single-5G</i>	Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.		
	<i>dual-5G</i>	Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.		
type	WTP, FortiAP or AP platform type. There are built-in WTP profiles for all supported FortiAP models. You can select a built-in profile and customize it or create a new profile.	option	-	221E
	Option	Description		
	<i>AP-11N</i>	Default 11n AP.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>C24JE</i>	FAPC24JE.		
	<i>421E</i>	FAP421E.		
	<i>423E</i>	FAP423E.		
	<i>221E</i>	FAP221E.		
	<i>222E</i>	FAP222E.		
	<i>223E</i>	FAP223E.		
	<i>224E</i>	FAP224E.		
	<i>231E</i>	FAP231E.		
	<i>321E</i>	FAP321E.		
	<i>431F</i>	FAP431F.		
	<i>431FL</i>	FAP431FL.		
	<i>432F</i>	FAP432F.		
	<i>432FR</i>	FAP432FR.		
	<i>433F</i>	FAP433F.		
	<i>433FL</i>	FAP433FL.		
	<i>231F</i>	FAP231F.		
	<i>231FL</i>	FAP231FL.		
	<i>234F</i>	FAP234F.		
	<i>23JF</i>	FAP23JF.		
	<i>831F</i>	FAP831F.		
	<i>231G</i>	FAP231G.		
	<i>233G</i>	FAP233G.		
	<i>234G</i>	FAP234G.		
	<i>431G</i>	FAP431G.		
	<i>432G</i>	FAP432G.		
	<i>433G</i>	FAP433G.		
	<i>231K</i>	FAP231K.		
	<i>23JK</i>	FAP23JK.		
	<i>241K</i>	FAP241K.		

Parameter	Description	Type	Size	Default
	Option	Description		
	243K	FAP243K.		
	441K	FAP441K.		
	443K	FAP443K.		
	U421E	FAPU421EV.		
	U422EV	FAPU422EV.		
	U423E	FAPU423EV.		
	U221EV	FAPU221EV.		
	U223EV	FAPU223EV.		
	U24JEV	FAPU24JEV.		
	U321EV	FAPU321EV.		
	U323EV	FAPU323EV.		
	U431F	FAPU431F.		
	U433F	FAPU433F.		
	U231F	FAPU231F.		
	U234F	FAPU234F.		
	U432F	FAPU432F.		
	U231G	FAPU231G.		

config radio-1

Parameter	Description	Type	Size	Default
80211d	Enable/disable 802.11d countryie (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable 802.11d countryie.		
	<i>disable</i>	Disable 802.11d countryie.		
80211mc	Enable/disable 802.11mc responder mode (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable 802.11mc responder mode.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable 802.11mc responder mode.</td></tr></table>	Option	Description	<i>disable</i>	Disable 802.11mc responder mode.													
Option	Description																	
<i>disable</i>	Disable 802.11mc responder mode.																	
airtime-fairness	Enable/disable airtime fairness (default = disable).	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td><i>disable</i></td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.											
Option	Description																	
<i>enable</i>	Enable airtime fairness (ATF) support.																	
<i>disable</i>	Disable airtime fairness (ATF) support.																	
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients (default = enable).	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AMSDU support.</td></tr><tr><td><i>disable</i></td><td>Disable AMSDU support.</td></tr></table>	Option	Description	<i>enable</i>	Enable AMSDU support.	<i>disable</i>	Disable AMSDU support.											
Option	Description																	
<i>enable</i>	Enable AMSDU support.																	
<i>disable</i>	Disable AMSDU support.																	
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00														
ap-sniffer-bufsize	Sniffer buffer size (1 - 32 MB, default = 16).	integer	Minimum value: 1 Maximum value: 32	16														
ap-sniffer-chan	Channel on which to operate the sniffer (default = 6).	integer	Minimum value: 0 Maximum value: 4294967295	36														
ap-sniffer-chan-width	Channel bandwidth for sniffer.	option	-	20MHz														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>320MHz</i></td><td>320 MHz channel width.</td></tr><tr><td><i>240MHz</i></td><td>240 MHz channel width.</td></tr><tr><td><i>160MHz</i></td><td>160 MHz channel width.</td></tr><tr><td><i>80MHz</i></td><td>80 MHz channel width.</td></tr><tr><td><i>40MHz</i></td><td>40 MHz channel width.</td></tr><tr><td><i>20MHz</i></td><td>20 MHz channel width.</td></tr></table>	Option	Description	<i>320MHz</i>	320 MHz channel width.	<i>240MHz</i>	240 MHz channel width.	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description																	
<i>320MHz</i>	320 MHz channel width.																	
<i>240MHz</i>	240 MHz channel width.																	
<i>160MHz</i>	160 MHz channel width.																	
<i>80MHz</i>	80 MHz channel width.																	
<i>40MHz</i>	40 MHz channel width.																	
<i>20MHz</i>	20 MHz channel width.																	

Parameter	Description	Type	Size	Default						
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi control frame.									
<i>disable</i>	Disable sniffer on WiFi control frame.									
ap-sniffer-data	Enable/disable sniffer on WiFi data frame (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi data frame									
<i>disable</i>	Disable sniffer on WiFi data frame									
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management other frame.									
<i>disable</i>	Disable sniffer on WiFi management other frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management probe frame.									
<i>disable</i>	Enable sniffer on WiFi management probe frame.									
arp-profile	Distributed Automatic Radio Resource Provisioning (DARRP) profile name to assign to the radio.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default																												
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17																												
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-	disable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable automatic transmit power adjustment.</td></tr><tr><td>disable</td><td>Disable automatic transmit power adjustment.</td></tr></table>				Option	Description	enable	Enable automatic transmit power adjustment.	disable	Disable automatic transmit power adjustment.																						
Option	Description																															
enable	Enable automatic transmit power adjustment.																															
disable	Disable automatic transmit power adjustment.																															
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10																												
auto-power-target	Target of automatic transmit power adjustment in dBm (-95 to -20, default = -70).	string	Maximum length: 7	-70																												
band	WiFi band that Radio 1 operates on.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g.</td></tr><tr><td>802.11n-2G</td><td>802.11n (WiFi 4) at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n (WiFi 4) at 5GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac (WiFi 5) at 2.4GHz.</td></tr><tr><td>802.11ac-5G</td><td>802.11ac (WiFi 5) at 5GHz.</td></tr><tr><td>802.11ax-2G</td><td>802.11ax (WiFi 6) at 2.4GHz.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax (WiFi 6) at 5GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax (WiFi 6) at 6GHz.</td></tr><tr><td>802.11be-2G</td><td>802.11be (WiFi 7) at 2.4GHz.</td></tr><tr><td>802.11be-5G</td><td>802.11be (WiFi 7) at 5GHz.</td></tr><tr><td>802.11be-6G</td><td>802.11be (WiFi 7) at 6GHz.</td></tr></table>				Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g.	802.11n-2G	802.11n (WiFi 4) at 2.4GHz.	802.11n-5G	802.11n (WiFi 4) at 5GHz.	802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.	802.11ac-5G	802.11ac (WiFi 5) at 5GHz.	802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.	802.11ax-5G	802.11ax (WiFi 6) at 5GHz.	802.11ax-6G	802.11ax (WiFi 6) at 6GHz.	802.11be-2G	802.11be (WiFi 7) at 2.4GHz.	802.11be-5G	802.11be (WiFi 7) at 5GHz.	802.11be-6G	802.11be (WiFi 7) at 6GHz.
Option	Description																															
802.11a	802.11a.																															
802.11b	802.11b.																															
802.11g	802.11g.																															
802.11n-2G	802.11n (WiFi 4) at 2.4GHz.																															
802.11n-5G	802.11n (WiFi 4) at 5GHz.																															
802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.																															
802.11ac-5G	802.11ac (WiFi 5) at 5GHz.																															
802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.																															
802.11ax-5G	802.11ax (WiFi 6) at 5GHz.																															
802.11ax-6G	802.11ax (WiFi 6) at 6GHz.																															
802.11be-2G	802.11be (WiFi 7) at 2.4GHz.																															
802.11be-5G	802.11be (WiFi 7) at 5GHz.																															
802.11be-6G	802.11be (WiFi 7) at 6GHz.																															

Parameter	Description	Type	Size	Default								
band-5g-type	WiFi 5G band type.	option	-	5g-full								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.			
Option	Description											
5g-full	Full 5G band.											
5g-high	High 5G band.											
5g-low	Low 5G band.											
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WMM bandwidth admission control.</td></tr><tr><td>disable</td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	enable	Enable WMM bandwidth admission control.	disable	Disable WMM bandwidth admission control.					
Option	Description											
enable	Enable WMM bandwidth admission control.											
disable	Disable WMM bandwidth admission control.											
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 1 Maximum value: 600000	2000								
beacon-interval	Beacon interval. The time between beacon frames in milliseconds. Actual range of beacon interval depends on the AP platform type (default = 100).	integer	Minimum value: 0 Maximum value: 65535	100								
bss-color	BSS color value for this 11ax radio (0 - 63, disable = 0, default = 0).	integer	Minimum value: 0 Maximum value: 63	0								
bss-color-mode	BSS color mode for this 11ax radio (default = auto).	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Automatically select BSS color value on AP.</td></tr><tr><td>static</td><td>Set BSS color value on this radio based on 'bss-color' CLI.</td></tr></table>	Option	Description	auto	Automatically select BSS color value on AP.	static	Set BSS color value on this radio based on 'bss-color' CLI.					
Option	Description											
auto	Automatically select BSS color value on AP.											
static	Set BSS color value on this radio based on 'bss-color' CLI.											

Parameter	Description	Type	Size	Default														
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.											
Option	Description																	
<i>enable</i>	Enable WMM call admission control.																	
<i>disable</i>	Disable WMM call admission control.																	
call-capacity	Maximum number of Voice over WLAN (VoWLAN) phones supported by the radio (0 - 60, default = 10).	integer	Minimum value: 10 0 Maximum value: 60															
channel<chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3															
channel-bonding	Channel bandwidth: 320, 240, 160, 80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>320MHz</i></td><td>320 MHz channel width.</td></tr><tr><td><i>240MHz</i></td><td>240 MHz channel width.</td></tr><tr><td><i>160MHz</i></td><td>160 MHz channel width.</td></tr><tr><td><i>80MHz</i></td><td>80 MHz channel width.</td></tr><tr><td><i>40MHz</i></td><td>40 MHz channel width.</td></tr><tr><td><i>20MHz</i></td><td>20 MHz channel width.</td></tr></table>	Option	Description	<i>320MHz</i>	320 MHz channel width.	<i>240MHz</i>	240 MHz channel width.	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description																	
<i>320MHz</i>	320 MHz channel width.																	
<i>240MHz</i>	240 MHz channel width.																	
<i>160MHz</i>	160 MHz channel width.																	
<i>80MHz</i>	80 MHz channel width.																	
<i>40MHz</i>	40 MHz channel width.																	
<i>20MHz</i>	20 MHz channel width.																	
channel-bonding-ext	Channel bandwidth extension: 320 MHz-1 and 320 MHz-2 (default = 320 MHz-2).	option	-	320MHz-2														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>320MHz-1</i></td><td>320 MHz channel with channel center frequency numbered 31, 95, and 159.</td></tr><tr><td><i>320MHz-2</i></td><td>320 MHz channel with channel center frequency numbered 63, 127, and 191.</td></tr></table>	Option	Description	<i>320MHz-1</i>	320 MHz channel with channel center frequency numbered 31, 95, and 159.	<i>320MHz-2</i>	320 MHz channel with channel center frequency numbered 63, 127, and 191.											
Option	Description																	
<i>320MHz-1</i>	320 MHz channel with channel center frequency numbered 31, 95, and 159.																	
<i>320MHz-2</i>	320 MHz channel with channel center frequency numbered 63, 127, and 191.																	

Parameter	Description	Type	Size	Default								
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable measuring channel utilization.</td></tr><tr><td><i>disable</i></td><td>Disable measuring channel utilization.</td></tr></table>	Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.					
Option	Description											
<i>enable</i>	Enable measuring channel utilization.											
<i>disable</i>	Disable measuring channel utilization.											
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support for both HT20 and HT40 on the same radio.</td></tr><tr><td><i>disable</i></td><td>Disable support for both HT20 and HT40 on the same radio.</td></tr></table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.					
Option	Description											
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.											
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.											
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is always using the most optimal channel (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distributed automatic radio resource provisioning.</td></tr><tr><td><i>disable</i></td><td>Disable distributed automatic radio resource provisioning.</td></tr></table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.					
Option	Description											
<i>enable</i>	Enable distributed automatic radio resource provisioning.											
<i>disable</i>	Disable distributed automatic radio resource provisioning.											
drma	Enable/disable dynamic radio mode assignment (DRMA) (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dynamic radio mode assignment (DRMA).</td></tr><tr><td><i>enable</i></td><td>Enable dynamic radio mode assignment (DRMA).</td></tr></table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).					
Option	Description											
<i>disable</i>	Disable dynamic radio mode assignment (DRMA).											
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).											
drma-sensitivity	Network Coverage Factor (NCF) percentage required to consider a radio as redundant (default = low).	option	-	low								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Consider a radio as redundant when its NCF is 100%.</td></tr><tr><td><i>medium</i></td><td>Consider a radio as redundant when its NCF is 95%.</td></tr><tr><td><i>high</i></td><td>Consider a radio as redundant when its NCF is 90%.</td></tr></table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.			
Option	Description											
<i>low</i>	Consider a radio as redundant when its NCF is 100%.											
<i>medium</i>	Consider a radio as redundant when its NCF is 95%.											
<i>high</i>	Consider a radio as redundant when its NCF is 90%.											

Parameter	Description	Type	Size	Default														
dtim	Delivery Traffic Indication Map (DTIM) period (1 - 255, default = 1). Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255															
frag-threshold	Maximum packet size that can be sent without fragmentation (800 - 2346 bytes, default = 2346).	integer	Minimum value: 800 Maximum value: 2346	2346														
iperf-protocol	Iperf test protocol (default = "UDP").	option	-	udp														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>UDP.</td></tr><tr><td>tcp</td><td>TCP.</td></tr></table>				Option	Description	udp	UDP.	tcp	TCP.								
Option	Description																	
udp	UDP.																	
tcp	TCP.																	
iperf-server-port	Iperf service port number.	integer	Minimum value: 5001 Maximum value: 65535															
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295															
max-distance	Maximum expected distance between the AP and clients (0 - 54000 m, default = 0).	integer	Minimum value: 0 Maximum value: 54000															
mimo-mode	Configure radio MIMO mode (default = default).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Default radio MIMO mode.</td></tr><tr><td>1x1</td><td>1x1 radio MIMO mode.</td></tr><tr><td>2x2</td><td>2x2 radio MIMO mode.</td></tr><tr><td>3x3</td><td>3x3 radio MIMO mode.</td></tr><tr><td>4x4</td><td>4x4 radio MIMO mode.</td></tr><tr><td>8x8</td><td>8x8 radio MIMO mode.</td></tr></table>				Option	Description	default	Default radio MIMO mode.	1x1	1x1 radio MIMO mode.	2x2	2x2 radio MIMO mode.	3x3	3x3 radio MIMO mode.	4x4	4x4 radio MIMO mode.	8x8	8x8 radio MIMO mode.
Option	Description																	
default	Default radio MIMO mode.																	
1x1	1x1 radio MIMO mode.																	
2x2	2x2 radio MIMO mode.																	
3x3	3x3 radio MIMO mode.																	
4x4	4x4 radio MIMO mode.																	
8x8	8x8 radio MIMO mode.																	
mode	Mode of radio 1. Radio 1 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap														

Parameter	Description	Type	Size	Default

Option		Description		
<i>disabled</i>		Radio 1 is disabled.		
<i>ap</i>		Radio 1 operates as an access point that allows WiFi clients to connect to your network.		
<i>monitor</i>		Radio 1 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.		
<i>sniffer</i>		Radio 1 operates as a sniffer capturing WiFi frames on air.		
<i>sam</i>		Radio 1 operates as a station that can connect to a neighboring AP for connectivity and health check.		

optional-antenna	Optional antenna used on FAP (default = none).	option	-	none

Option		Description		
<i>none</i>		None.		
<i>custom</i>		Customize optional antenna gain.		
<i>FANT-04ABGN-0606-O-N</i>		6 dBi(2.4GHz) and 6 dBi(5GHz).		
<i>FANT-04ABGN-1414-P-N</i>		14 dBi(2.4GHz) and 14 dBi(5GHz).		
<i>FANT-04ABGN-8065-P-N</i>		8 dBi(2.4GHz) and 6.5 dBi(5GHz).		
<i>FANT-04ABGN-0606-O-R</i>		6 dBi(2.4GHz) and 6 dBi(5GHz).		
<i>FANT-04ABGN-0606-P-R</i>		6 dBi(2.4GHz) and 6 dBi(5GHz).		
<i>FANT-10ACAX-1213-D-N</i>		12 dBi(2.4GHz) and 13 dBi(5GHz).		
<i>FANT-08ABGN-1213-D-R</i>		12 dBi(2.4GHz) and 13 dBi(5GHz).		

Parameter	Description	Type	Size	Default												
optional-antenna-gain	Optional antenna gain in dBi (0 to 20, default = 0).	string	Maximum length: 7	0												
power-level	Radio EIRP power level as a percentage of the maximum EIRP power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100	100												
power-mode	Set radio effective isotropic radiated power (EIRP) in dBm or by a percentage of the maximum EIRP (default = percentage). This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>				Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.						
Option	Description															
<i>dBm</i>	Set radio EIRP power in dBm.															
<i>percentage</i>	Set radio EIRP power by percentage.															
power-value	Radio EIRP power in dBm (1 - 33, default = 27).	integer	Minimum value: 1 Maximum value: 33	27												
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tim</i></td><td>TIM bit for client in power save mode.</td></tr><tr><td><i>ac-vo</i></td><td>Use AC VO priority to send out packets in the power save queue.</td></tr><tr><td><i>no-obss-scan</i></td><td>Do not put OBSS scan IE into beacon and probe response frames.</td></tr><tr><td><i>no-11b-rate</i></td><td>Do not send frame using 11b data rate.</td></tr><tr><td><i>client-rate-follow</i></td><td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td></tr></table>				Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.
Option	Description															
<i>tim</i>	TIM bit for client in power save mode.															
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.															
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.															
<i>no-11b-rate</i>	Do not send frame using 11b data rate.															
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.															
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rtscts</i></td><td>Enable 802.11g protection RTS/CTS mode.</td></tr></table>				Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.								
Option	Description															
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.		
	<i>disable</i>	Disable 802.11g protection mode.		
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS (256 - 2346 bytes, default = 2346).	integer	Minimum value: 256 Maximum value: 2346	2346
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00
sam-ca-certificate	CA certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 79	
sam-captive-portal	Enable/disable Captive Portal Authentication (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Captive Portal Authentication.		
	<i>disable</i>	Disable Captive Portal Authentication.		
sam-client-certificate	Client certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35	
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64	
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64	
sam-cwp-password	Password for captive portal authentication.	password	Not Specified	
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64	
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255	
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35	
sam-eap-method	Select WPA2/WPA3-ENTERPRISE EAP Method (default = PEAP).	option	-	peap

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>both</i></td><td>EAP PEAP and TLS. (Not applicable in FIPS mode)</td></tr><tr><td><i>tls</i></td><td>EAP TLS.</td></tr><tr><td><i>peap</i></td><td>EAP PEAP. (Not applicable in FIPS mode)</td></tr></table>	Option	Description	<i>both</i>	EAP PEAP and TLS. (Not applicable in FIPS mode)	<i>tls</i>	EAP TLS.	<i>peap</i>	EAP PEAP. (Not applicable in FIPS mode)							
	Option	Description														
	<i>both</i>	EAP PEAP and TLS. (Not applicable in FIPS mode)														
	<i>tls</i>	EAP TLS.														
<i>peap</i>	EAP PEAP. (Not applicable in FIPS mode)															
sam-password	Passphrase for WiFi network connection.	password	Not Specified													
sam-private-key	Private key for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35													
sam-private-key-password	Password for private key file for WPA2/WPA3-ENTERPRISE.	password	Not Specified													
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 0 60 Maximum value: 864000													
sam-security-type	Select WiFi network security type (default = "wpa-personal" for 2.4/5G radio, "wpa3-sae" for 6G radio).	option	-	wpa-personal												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA/WPA2 personal.</td></tr><tr><td><i>wpa-enterprise</i></td><td>WPA2/WPA3 enterprise.</td></tr><tr><td><i>wpa3-sae</i></td><td>WPA3 SAE.</td></tr><tr><td><i>owe</i></td><td>OWE.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-enterprise</i>	WPA2/WPA3 enterprise.	<i>wpa3-sae</i>	WPA3 SAE.	<i>owe</i>	OWE.			
	Option	Description														
	<i>open</i>	Open.														
	<i>wpa-personal</i>	WPA/WPA2 personal.														
	<i>wpa-enterprise</i>	WPA2/WPA3 enterprise.														
	<i>wpa3-sae</i>	WPA3 SAE.														
<i>owe</i>	OWE.															
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255													
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0												
sam-server-type	Select SAM server type (default = "IP").	option	-	ip												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Fully Qualified Domain Name address.</td></tr></table>	Option	Description	<i>ip</i>	IPv4 address.	<i>fqdn</i>	Fully Qualified Domain Name address.									
	Option	Description														
	<i>ip</i>	IPv4 address.														
<i>fqdn</i>	Fully Qualified Domain Name address.															
sam-ssid	SSID for WiFi network.	string	Maximum length: 32													

Parameter	Description	Type	Size	Default												
sam-test	Select SAM test type (default = "PING").	option	-	ping												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING test.</td></tr><tr><td>iperf</td><td>IPERF test.</td></tr></table>	Option	Description	ping	PING test.	iperf	IPERF test.									
Option	Description															
ping	PING test.															
iperf	IPERF test.															
sam-username	Username for WiFi network connection.	string	Maximum length: 35													
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td>disable</td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>	Option	Description	enable	Select the 400 ns short guard interval (Short GI).	disable	Select the 800 ns long guard interval (Long GI).									
Option	Description															
enable	Select the 400 ns short guard interval (Short GI).															
disable	Select the 800 ns long guard interval (Long GI).															
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable packet transmission optimization.</td></tr><tr><td>power-save</td><td>Tag client as operating in power save mode if excessive transmit retries occur.</td></tr><tr><td>aggr-limit</td><td>Set aggregation limit to a lower value when data rate is low.</td></tr><tr><td>retry-limit</td><td>Set software retry limit to a lower value when data rate is low.</td></tr><tr><td>send-bar</td><td>Limit transmission of BAR frames.</td></tr></table>	Option	Description	disable	Disable packet transmission optimization.	power-save	Tag client as operating in power save mode if excessive transmit retries occur.	aggr-limit	Set aggregation limit to a lower value when data rate is low.	retry-limit	Set software retry limit to a lower value when data rate is low.	send-bar	Limit transmission of BAR frames.			
Option	Description															
disable	Disable packet transmission optimization.															
power-save	Tag client as operating in power save mode if excessive transmit retries occur.															
aggr-limit	Set aggregation limit to a lower value when data rate is low.															
retry-limit	Set software retry limit to a lower value when data rate is low.															
send-bar	Limit transmission of BAR frames.															
vap-all	Configure method for assigning SSIDs to this FortiAP (default = automatically assign tunnel SSIDs).	option	-	tunnel												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tunnel</td><td>Automatically select tunnel SSIDs.</td></tr><tr><td>bridge</td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td>manual</td><td>Manually select SSIDs.</td></tr></table>	Option	Description	tunnel	Automatically select tunnel SSIDs.	bridge	Automatically select local-bridging SSIDs.	manual	Manually select SSIDs.							
Option	Description															
tunnel	Automatically select tunnel SSIDs.															
bridge	Automatically select local-bridging SSIDs.															
manual	Manually select SSIDs.															
vaps <name>	Manually selected list of Virtual Access Points (VAPs).	string	Maximum length: 35													

Parameter	Description	Type	Size	Default						
	Virtual Access Point (VAP) name.									
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35							
zero-wait-dfs	Enable/disable zero wait DFS on radio (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero wait DFS</td></tr><tr><td><i>disable</i></td><td>Disable zero wait DFS</td></tr></table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS			
Option	Description									
<i>enable</i>	Enable zero wait DFS									
<i>disable</i>	Disable zero wait DFS									

config radio-2

Parameter	Description	Type	Size	Default						
80211d	Enable/disable 802.11d countryie (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11d countryie.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11d countryie.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11d countryie.	<i>disable</i>	Disable 802.11d countryie.			
Option	Description									
<i>enable</i>	Enable 802.11d countryie.									
<i>disable</i>	Disable 802.11d countryie.									
80211mc	Enable/disable 802.11mc responder mode (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11mc responder mode.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11mc responder mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11mc responder mode.	<i>disable</i>	Disable 802.11mc responder mode.			
Option	Description									
<i>enable</i>	Enable 802.11mc responder mode.									
<i>disable</i>	Disable 802.11mc responder mode.									
airtime-fairness	Enable/disable airtime fairness (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td><i>disable</i></td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.			
Option	Description									
<i>enable</i>	Enable airtime fairness (ATF) support.									
<i>disable</i>	Disable airtime fairness (ATF) support.									
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients (default = enable).	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00
ap-sniffer-bufsize	Sniffer buffer size (1 - 32 MB, default = 16).	integer	Minimum value: 1 Maximum value: 32	16
ap-sniffer-chan	Channel on which to operate the sniffer (default = 6).	integer	Minimum value: 0 Maximum value: 4294967295	6
ap-sniffer-chan-width	Channel bandwidth for sniffer.	option	-	20MHz
	Option Description			
	<i>320MHz</i>	320 MHz channel width.		
	<i>240MHz</i>	240 MHz channel width.		
	<i>160MHz</i>	160 MHz channel width.		
	<i>80MHz</i>	80 MHz channel width.		
	<i>40MHz</i>	40 MHz channel width.		
	<i>20MHz</i>	20 MHz channel width.		
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable sniffer on WiFi control frame.		
	<i>disable</i>	Disable sniffer on WiFi control frame.		
ap-sniffer-data	Enable/disable sniffer on WiFi data frame (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable sniffer on WiFi data frame		
	<i>disable</i>	Disable sniffer on WiFi data frame		

Parameter	Description	Type	Size	Default						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management other frame.									
<i>disable</i>	Disable sniffer on WiFi management other frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management probe frame.									
<i>disable</i>	Enable sniffer on WiFi management probe frame.									
arrp-profile	Distributed Automatic Radio Resource Provisioning (DARRP) profile name to assign to the radio.	string	Maximum length: 35							
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 17 0 Maximum value: 4294967295							
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									

Parameter	Description	Type	Size	Default																												
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 10 0 Maximum value: 4294967295																													
auto-power-target	Target of automatic transmit power adjustment in dBm (-95 to -20, default = -70).	string	Maximum length: 7	-70																												
band	WiFi band that Radio 2 operates on.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g.</td></tr><tr><td>802.11n-2G</td><td>802.11n (WiFi 4) at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n (WiFi 4) at 5GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac (WiFi 5) at 2.4GHz.</td></tr><tr><td>802.11ac-5G</td><td>802.11ac (WiFi 5) at 5GHz.</td></tr><tr><td>802.11ax-2G</td><td>802.11ax (WiFi 6) at 2.4GHz.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax (WiFi 6) at 5GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax (WiFi 6) at 6GHz.</td></tr><tr><td>802.11be-2G</td><td>802.11be (WiFi 7) at 2.4GHz.</td></tr><tr><td>802.11be-5G</td><td>802.11be (WiFi 7) at 5GHz.</td></tr><tr><td>802.11be-6G</td><td>802.11be (WiFi 7) at 6GHz.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g.	802.11n-2G	802.11n (WiFi 4) at 2.4GHz.	802.11n-5G	802.11n (WiFi 4) at 5GHz.	802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.	802.11ac-5G	802.11ac (WiFi 5) at 5GHz.	802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.	802.11ax-5G	802.11ax (WiFi 6) at 5GHz.	802.11ax-6G	802.11ax (WiFi 6) at 6GHz.	802.11be-2G	802.11be (WiFi 7) at 2.4GHz.	802.11be-5G	802.11be (WiFi 7) at 5GHz.	802.11be-6G	802.11be (WiFi 7) at 6GHz.			
Option	Description																															
802.11a	802.11a.																															
802.11b	802.11b.																															
802.11g	802.11g.																															
802.11n-2G	802.11n (WiFi 4) at 2.4GHz.																															
802.11n-5G	802.11n (WiFi 4) at 5GHz.																															
802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.																															
802.11ac-5G	802.11ac (WiFi 5) at 5GHz.																															
802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.																															
802.11ax-5G	802.11ax (WiFi 6) at 5GHz.																															
802.11ax-6G	802.11ax (WiFi 6) at 6GHz.																															
802.11be-2G	802.11be (WiFi 7) at 2.4GHz.																															
802.11be-5G	802.11be (WiFi 7) at 5GHz.																															
802.11be-6G	802.11be (WiFi 7) at 6GHz.																															
band-5g-type	WiFi 5G band type.	option	-	5g-full																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.																							
Option	Description																															
5g-full	Full 5G band.																															
5g-high	High 5G band.																															
5g-low	Low 5G band.																															

Parameter	Description	Type	Size	Default						
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 2000 1 Maximum value: 600000							
beacon-interval	Beacon interval. The time between beacon frames in milliseconds. Actual range of beacon interval depends on the AP platform type (default = 100).	integer	Minimum value: 100 0 Maximum value: 65535							
bss-color	BSS color value for this 11ax radio (0 - 63, disable = 0, default = 0).	integer	Minimum value: 0 0 Maximum value: 63							
bss-color-mode	BSS color mode for this 11ax radio (default = auto).	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically select BSS color value on AP.</td></tr><tr><td><i>static</i></td><td>Set BSS color value on this radio based on 'bss-color' CLI.</td></tr></table>	Option	Description	<i>auto</i>	Automatically select BSS color value on AP.	<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.			
Option	Description									
<i>auto</i>	Automatically select BSS color value on AP.									
<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.			
Option	Description									
<i>enable</i>	Enable WMM call admission control.									
<i>disable</i>	Disable WMM call admission control.									

Parameter	Description	Type	Size	Default														
call-capacity	Maximum number of Voice over WLAN (VoWLAN) phones supported by the radio (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60	10														
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3															
channel-bonding	Channel bandwidth: 320, 240, 160, 80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>320MHz</td><td>320 MHz channel width.</td></tr><tr><td>240MHz</td><td>240 MHz channel width.</td></tr><tr><td>160MHz</td><td>160 MHz channel width.</td></tr><tr><td>80MHz</td><td>80 MHz channel width.</td></tr><tr><td>40MHz</td><td>40 MHz channel width.</td></tr><tr><td>20MHz</td><td>20 MHz channel width.</td></tr></table>				Option	Description	320MHz	320 MHz channel width.	240MHz	240 MHz channel width.	160MHz	160 MHz channel width.	80MHz	80 MHz channel width.	40MHz	40 MHz channel width.	20MHz	20 MHz channel width.
Option	Description																	
320MHz	320 MHz channel width.																	
240MHz	240 MHz channel width.																	
160MHz	160 MHz channel width.																	
80MHz	80 MHz channel width.																	
40MHz	40 MHz channel width.																	
20MHz	20 MHz channel width.																	
channel-bonding-ext	Channel bandwidth extension: 320 MHz-1 and 320 MHz-2 (default = 320 MHz-2).	option	-	320MHz-2														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>320MHz-1</td><td>320 MHz channel with channel center frequency numbered 31, 95, and 159.</td></tr><tr><td>320MHz-2</td><td>320 MHz channel with channel center frequency numbered 63, 127, and 191.</td></tr></table>				Option	Description	320MHz-1	320 MHz channel with channel center frequency numbered 31, 95, and 159.	320MHz-2	320 MHz channel with channel center frequency numbered 63, 127, and 191.								
Option	Description																	
320MHz-1	320 MHz channel with channel center frequency numbered 31, 95, and 159.																	
320MHz-2	320 MHz channel with channel center frequency numbered 63, 127, and 191.																	
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable measuring channel utilization.</td></tr><tr><td>disable</td><td>Disable measuring channel utilization.</td></tr></table>				Option	Description	enable	Enable measuring channel utilization.	disable	Disable measuring channel utilization.								
Option	Description																	
enable	Enable measuring channel utilization.																	
disable	Disable measuring channel utilization.																	
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).	option	-	enable														

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>			Enable support for both HT20 and HT40 on the same radio.
	<i>disable</i>			Disable support for both HT20 and HT40 on the same radio.
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is always using the most optimal channel (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>			Enable distributed automatic radio resource provisioning.
	<i>disable</i>			Disable distributed automatic radio resource provisioning.
drma	Enable/disable dynamic radio mode assignment (DRMA) (default = disable).	option	-	disable
	Option Description			
	<i>disable</i>			Disable dynamic radio mode assignment (DRMA).
	<i>enable</i>			Enable dynamic radio mode assignment (DRMA).
drma-sensitivity	Network Coverage Factor (NCF) percentage required to consider a radio as redundant (default = low).	option	-	low
	Option Description			
	<i>low</i>			Consider a radio as redundant when its NCF is 100%.
	<i>medium</i>			Consider a radio as redundant when its NCF is 95%.
	<i>high</i>			Consider a radio as redundant when its NCF is 90%.
dtim	Delivery Traffic Indication Map (DTIM) period (1 - 255, default = 1). Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	
frag-threshold	Maximum packet size that can be sent without fragmentation (800 - 2346 bytes, default = 2346).	integer	Minimum value: 800 Maximum value: 2346	
iperf-protocol	Iperf test protocol (default = "UDP").	option	-	udp

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>UDP.</td></tr><tr><td>tcp</td><td>TCP.</td></tr></table>	Option	Description	udp	UDP.	tcp	TCP.											
	Option	Description																
	udp	UDP.																
tcp	TCP.																	
iperf-server-port	Iperf service port number.	integer	Minimum value: 5001 0 Maximum value: 65535															
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 0 Maximum value: 4294967295															
max-distance	Maximum expected distance between the AP and clients (0 - 54000 m, default = 0).	integer	Minimum value: 0 0 Maximum value: 54000															
mimo-mode	Configure radio MIMO mode (default = default).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Default radio MIMO mode.</td></tr><tr><td>1x1</td><td>1x1 radio MIMO mode.</td></tr><tr><td>2x2</td><td>2x2 radio MIMO mode.</td></tr><tr><td>3x3</td><td>3x3 radio MIMO mode.</td></tr><tr><td>4x4</td><td>4x4 radio MIMO mode.</td></tr><tr><td>8x8</td><td>8x8 radio MIMO mode.</td></tr></table>	Option	Description	default	Default radio MIMO mode.	1x1	1x1 radio MIMO mode.	2x2	2x2 radio MIMO mode.	3x3	3x3 radio MIMO mode.	4x4	4x4 radio MIMO mode.	8x8	8x8 radio MIMO mode.			
	Option	Description																
	default	Default radio MIMO mode.																
	1x1	1x1 radio MIMO mode.																
	2x2	2x2 radio MIMO mode.																
	3x3	3x3 radio MIMO mode.																
	4x4	4x4 radio MIMO mode.																
8x8	8x8 radio MIMO mode.																	
mode	Mode of radio 2. Radio 2 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disabled</td><td>Radio 2 is disabled.</td></tr><tr><td>ap</td><td>Radio 2 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td>monitor</td><td>Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr></table>	Option	Description	disabled	Radio 2 is disabled.	ap	Radio 2 operates as an access point that allows WiFi clients to connect to your network.	monitor	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.									
	Option	Description																
	disabled	Radio 2 is disabled.																
ap	Radio 2 operates as an access point that allows WiFi clients to connect to your network.																	
monitor	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																	

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sniffer</i></td><td>Radio 2 operates as a sniffer capturing WiFi frames on air.</td></tr><tr><td><i>sam</i></td><td>Radio 2 operates as a station that can connect to a neighboring AP for connectivity and health check.</td></tr></table>	Option	Description	<i>sniffer</i>	Radio 2 operates as a sniffer capturing WiFi frames on air.	<i>sam</i>	Radio 2 operates as a station that can connect to a neighboring AP for connectivity and health check.																	
	Option	Description																						
	<i>sniffer</i>	Radio 2 operates as a sniffer capturing WiFi frames on air.																						
<i>sam</i>	Radio 2 operates as a station that can connect to a neighboring AP for connectivity and health check.																							
optional-antenna	Optional antenna used on FAP (default = none).	option	-	none																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>custom</i></td><td>Customize optional antenna gain.</td></tr><tr><td><i>FANT-04ABGN-0606-O-N</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-1414-P-N</i></td><td>14 dBi(2.4GHz) and 14 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-8065-P-N</i></td><td>8 dBi(2.4GHz) and 6.5 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-0606-O-R</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-0606-P-R</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-10ACAX-1213-D-N</i></td><td>12 dBi(2.4GHz) and 13 dBi(5GHz).</td></tr><tr><td><i>FANT-08ABGN-1213-D-R</i></td><td>12 dBi(2.4GHz) and 13 dBi(5GHz).</td></tr></table>	Option	Description	<i>none</i>	None.	<i>custom</i>	Customize optional antenna gain.	<i>FANT-04ABGN-0606-O-N</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-04ABGN-1414-P-N</i>	14 dBi(2.4GHz) and 14 dBi(5GHz).	<i>FANT-04ABGN-8065-P-N</i>	8 dBi(2.4GHz) and 6.5 dBi(5GHz).	<i>FANT-04ABGN-0606-O-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-04ABGN-0606-P-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-10ACAX-1213-D-N</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).	<i>FANT-08ABGN-1213-D-R</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).			
	Option	Description																						
	<i>none</i>	None.																						
	<i>custom</i>	Customize optional antenna gain.																						
	<i>FANT-04ABGN-0606-O-N</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-04ABGN-1414-P-N</i>	14 dBi(2.4GHz) and 14 dBi(5GHz).																						
	<i>FANT-04ABGN-8065-P-N</i>	8 dBi(2.4GHz) and 6.5 dBi(5GHz).																						
	<i>FANT-04ABGN-0606-O-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-04ABGN-0606-P-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-10ACAX-1213-D-N</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).																						
<i>FANT-08ABGN-1213-D-R</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).																							
optional-antenna-gain	Optional antenna gain in dBi (0 to 20, default = 0).	string	Maximum length: 7	0																				
power-level	Radio EIRP power level as a percentage of the maximum EIRP power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100	100																				

Parameter	Description	Type	Size	Default												
power-mode	Set radio effective isotropic radiated power (EIRP) in dBm or by a percentage of the maximum EIRP (default = percentage). This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.									
Option	Description															
<i>dBm</i>	Set radio EIRP power in dBm.															
<i>percentage</i>	Set radio EIRP power by percentage.															
power-value	Radio EIRP power in dBm (1 - 33, default = 27).	integer	Minimum value: 27 1 Maximum value: 33													
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tim</i></td><td>TIM bit for client in power save mode.</td></tr><tr><td><i>ac-vo</i></td><td>Use AC VO priority to send out packets in the power save queue.</td></tr><tr><td><i>no-obss-scan</i></td><td>Do not put OBSS scan IE into beacon and probe response frames.</td></tr><tr><td><i>no-11b-rate</i></td><td>Do not send frame using 11b data rate.</td></tr><tr><td><i>client-rate-follow</i></td><td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td></tr></table>	Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.			
Option	Description															
<i>tim</i>	TIM bit for client in power save mode.															
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.															
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.															
<i>no-11b-rate</i>	Do not send frame using 11b data rate.															
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.															
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rtscts</i></td><td>Enable 802.11g protection RTS/CTS mode.</td></tr><tr><td><i>ctsonly</i></td><td>Enable 802.11g protection CTS only mode.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11g protection mode.</td></tr></table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.							
Option	Description															
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.															
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.															
<i>disable</i>	Disable 802.11g protection mode.															

Parameter	Description	Type	Size	Default								
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS (256 - 2346 bytes, default = 2346).	integer	Minimum value: 256 Maximum value: 2346	2346								
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00								
sam-ca-certificate	CA certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 79									
sam-captive-portal	Enable/disable Captive Portal Authentication (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Captive Portal Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable Captive Portal Authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable Captive Portal Authentication.	<i>disable</i>	Disable Captive Portal Authentication.		
Option	Description											
<i>enable</i>	Enable Captive Portal Authentication.											
<i>disable</i>	Disable Captive Portal Authentication.											
sam-client-certificate	Client certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35									
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64									
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64									
sam-cwp-password	Password for captive portal authentication.	password	Not Specified									
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64									
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255									
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35									
sam-eap-method	Select WPA2/WPA3-ENTERPRISE EAP Method (default = PEAP).	option	-	peap								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>both</i></td><td>EAP PEAP and TLS. (Not applicable in FIPS mode)</td></tr><tr><td><i>tls</i></td><td>EAP TLS.</td></tr><tr><td><i>peap</i></td><td>EAP PEAP. (Not applicable in FIPS mode)</td></tr></table>				Option	Description	<i>both</i>	EAP PEAP and TLS. (Not applicable in FIPS mode)	<i>tls</i>	EAP TLS.	<i>peap</i>	EAP PEAP. (Not applicable in FIPS mode)
Option	Description											
<i>both</i>	EAP PEAP and TLS. (Not applicable in FIPS mode)											
<i>tls</i>	EAP TLS.											
<i>peap</i>	EAP PEAP. (Not applicable in FIPS mode)											

Parameter	Description	Type	Size	Default												
sam-password	Passphrase for WiFi network connection.	password	Not Specified													
sam-private-key	Private key for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35													
sam-private-key-password	Password for private key file for WPA2/WPA3-ENTERPRISE.	password	Not Specified													
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0												
sam-security-type	Select WiFi network security type (default = "wpa-personal" for 2.4/5G radio, "wpa3-sae" for 6G radio).	option	-	wpa-personal												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>open</td><td>Open.</td></tr><tr><td>wpa-personal</td><td>WPA/WPA2 personal.</td></tr><tr><td>wpa-enterprise</td><td>WPA2/WPA3 enterprise.</td></tr><tr><td>wpa3-sae</td><td>WPA3 SAE.</td></tr><tr><td>owe</td><td>OWE.</td></tr></table>				Option	Description	open	Open.	wpa-personal	WPA/WPA2 personal.	wpa-enterprise	WPA2/WPA3 enterprise.	wpa3-sae	WPA3 SAE.	owe	OWE.
Option	Description															
open	Open.															
wpa-personal	WPA/WPA2 personal.															
wpa-enterprise	WPA2/WPA3 enterprise.															
wpa3-sae	WPA3 SAE.															
owe	OWE.															
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255													
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0												
sam-server-type	Select SAM server type (default = "IP").	option	-	ip												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ip</td><td>IPv4 address.</td></tr><tr><td>fqdn</td><td>Fully Qualified Domain Name address.</td></tr></table>				Option	Description	ip	IPv4 address.	fqdn	Fully Qualified Domain Name address.						
Option	Description															
ip	IPv4 address.															
fqdn	Fully Qualified Domain Name address.															
sam-ssid	SSID for WiFi network.	string	Maximum length: 32													
sam-test	Select SAM test type (default = "PING").	option	-	ping												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING test.</td></tr></table>				Option	Description	ping	PING test.								
Option	Description															
ping	PING test.															

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>iperf</i></td><td>IPERF test.</td></tr></table>	Option	Description	<i>iperf</i>	IPERF test.											
Option	Description															
<i>iperf</i>	IPERF test.															
sam-username	Username for WiFi network connection.	string	Maximum length: 35													
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td><i>disable</i></td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).									
Option	Description															
<i>enable</i>	Select the 400 ns short guard interval (Short GI).															
<i>disable</i>	Select the 800 ns long guard interval (Long GI).															
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet transmission optimization.</td></tr><tr><td><i>power-save</i></td><td>Tag client as operating in power save mode if excessive transmit retries occur.</td></tr><tr><td><i>aggr-limit</i></td><td>Set aggregation limit to a lower value when data rate is low.</td></tr><tr><td><i>retry-limit</i></td><td>Set software retry limit to a lower value when data rate is low.</td></tr><tr><td><i>send-bar</i></td><td>Limit transmission of BAR frames.</td></tr></table>	Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.			
Option	Description															
<i>disable</i>	Disable packet transmission optimization.															
<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.															
<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.															
<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.															
<i>send-bar</i>	Limit transmission of BAR frames.															
vap-all	Configure method for assigning SSIDs to this FortiAP (default = automatically assign tunnel SSIDs).	option	-	tunnel												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.							
Option	Description															
<i>tunnel</i>	Automatically select tunnel SSIDs.															
<i>bridge</i>	Automatically select local-bridging SSIDs.															
<i>manual</i>	Manually select SSIDs.															
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35													

Parameter	Description	Type	Size	Default						
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35							
zero-wait-dfs	Enable/disable zero wait DFS on radio (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero wait DFS</td></tr><tr><td><i>disable</i></td><td>Disable zero wait DFS</td></tr></table>				Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS
Option	Description									
<i>enable</i>	Enable zero wait DFS									
<i>disable</i>	Disable zero wait DFS									

config radio-3

Parameter	Description	Type	Size	Default						
80211d	Enable/disable 802.11d countryie (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11d countryie.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11d countryie.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11d countryie.	<i>disable</i>	Disable 802.11d countryie.			
Option	Description									
<i>enable</i>	Enable 802.11d countryie.									
<i>disable</i>	Disable 802.11d countryie.									
80211mc	Enable/disable 802.11mc responder mode (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11mc responder mode.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11mc responder mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11mc responder mode.	<i>disable</i>	Disable 802.11mc responder mode.			
Option	Description									
<i>enable</i>	Enable 802.11mc responder mode.									
<i>disable</i>	Disable 802.11mc responder mode.									
airtime-fairness	Enable/disable airtime fairness (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td><i>disable</i></td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.			
Option	Description									
<i>enable</i>	Enable airtime fairness (ATF) support.									
<i>disable</i>	Disable airtime fairness (ATF) support.									
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients (default = enable).	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00
ap-sniffer-bufsize	Sniffer buffer size (1 - 32 MB, default = 16).	integer	Minimum value: 1 Maximum value: 32	16
ap-sniffer-chan	Channel on which to operate the sniffer (default = 6).	integer	Minimum value: 0 Maximum value: 4294967295	37
ap-sniffer-chan-width	Channel bandwidth for sniffer.	option	-	20MHz
	Option Description			
	<i>320MHz</i>	320 MHz channel width.		
	<i>240MHz</i>	240 MHz channel width.		
	<i>160MHz</i>	160 MHz channel width.		
	<i>80MHz</i>	80 MHz channel width.		
	<i>40MHz</i>	40 MHz channel width.		
	<i>20MHz</i>	20 MHz channel width.		
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable sniffer on WiFi control frame.		
	<i>disable</i>	Disable sniffer on WiFi control frame.		
ap-sniffer-data	Enable/disable sniffer on WiFi data frame (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable sniffer on WiFi data frame		
	<i>disable</i>	Disable sniffer on WiFi data frame		

Parameter	Description	Type	Size	Default						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management other frame.									
<i>disable</i>	Disable sniffer on WiFi management other frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management probe frame.									
<i>disable</i>	Enable sniffer on WiFi management probe frame.									
arrp-profile	Distributed Automatic Radio Resource Provisioning (DARRP) profile name to assign to the radio.	string	Maximum length: 35							
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 17 0 Maximum value: 4294967295							
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									

Parameter	Description	Type	Size	Default																												
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 10 0 Maximum value: 4294967295																													
auto-power-target	Target of automatic transmit power adjustment in dBm (-95 to -20, default = -70).	string	Maximum length: 7	-70																												
band	WiFi band that Radio 3 operates on.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g.</td></tr><tr><td>802.11n-2G</td><td>802.11n (WiFi 4) at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n (WiFi 4) at 5GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac (WiFi 5) at 2.4GHz.</td></tr><tr><td>802.11ac-5G</td><td>802.11ac (WiFi 5) at 5GHz.</td></tr><tr><td>802.11ax-2G</td><td>802.11ax (WiFi 6) at 2.4GHz.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax (WiFi 6) at 5GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax (WiFi 6) at 6GHz.</td></tr><tr><td>802.11be-2G</td><td>802.11be (WiFi 7) at 2.4GHz.</td></tr><tr><td>802.11be-5G</td><td>802.11be (WiFi 7) at 5GHz.</td></tr><tr><td>802.11be-6G</td><td>802.11be (WiFi 7) at 6GHz.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g.	802.11n-2G	802.11n (WiFi 4) at 2.4GHz.	802.11n-5G	802.11n (WiFi 4) at 5GHz.	802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.	802.11ac-5G	802.11ac (WiFi 5) at 5GHz.	802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.	802.11ax-5G	802.11ax (WiFi 6) at 5GHz.	802.11ax-6G	802.11ax (WiFi 6) at 6GHz.	802.11be-2G	802.11be (WiFi 7) at 2.4GHz.	802.11be-5G	802.11be (WiFi 7) at 5GHz.	802.11be-6G	802.11be (WiFi 7) at 6GHz.			
Option	Description																															
802.11a	802.11a.																															
802.11b	802.11b.																															
802.11g	802.11g.																															
802.11n-2G	802.11n (WiFi 4) at 2.4GHz.																															
802.11n-5G	802.11n (WiFi 4) at 5GHz.																															
802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.																															
802.11ac-5G	802.11ac (WiFi 5) at 5GHz.																															
802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.																															
802.11ax-5G	802.11ax (WiFi 6) at 5GHz.																															
802.11ax-6G	802.11ax (WiFi 6) at 6GHz.																															
802.11be-2G	802.11be (WiFi 7) at 2.4GHz.																															
802.11be-5G	802.11be (WiFi 7) at 5GHz.																															
802.11be-6G	802.11be (WiFi 7) at 6GHz.																															
band-5g-type	WiFi 5G band type.	option	-	5g-full																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.																							
Option	Description																															
5g-full	Full 5G band.																															
5g-high	High 5G band.																															
5g-low	Low 5G band.																															

Parameter	Description	Type	Size	Default						
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 2000 1 Maximum value: 600000							
beacon-interval	Beacon interval. The time between beacon frames in milliseconds. Actual range of beacon interval depends on the AP platform type (default = 100).	integer	Minimum value: 100 0 Maximum value: 65535							
bss-color	BSS color value for this 11ax radio (0 - 63, disable = 0, default = 0).	integer	Minimum value: 0 0 Maximum value: 63							
bss-color-mode	BSS color mode for this 11ax radio (default = auto).	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically select BSS color value on AP.</td></tr><tr><td><i>static</i></td><td>Set BSS color value on this radio based on 'bss-color' CLI.</td></tr></table>	Option	Description	<i>auto</i>	Automatically select BSS color value on AP.	<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.			
Option	Description									
<i>auto</i>	Automatically select BSS color value on AP.									
<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.			
Option	Description									
<i>enable</i>	Enable WMM call admission control.									
<i>disable</i>	Disable WMM call admission control.									

Parameter	Description	Type	Size	Default														
call-capacity	Maximum number of Voice over WLAN (VoWLAN) phones supported by the radio (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60	10														
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3															
channel-bonding	Channel bandwidth: 320, 240, 160, 80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>320MHz</td><td>320 MHz channel width.</td></tr><tr><td>240MHz</td><td>240 MHz channel width.</td></tr><tr><td>160MHz</td><td>160 MHz channel width.</td></tr><tr><td>80MHz</td><td>80 MHz channel width.</td></tr><tr><td>40MHz</td><td>40 MHz channel width.</td></tr><tr><td>20MHz</td><td>20 MHz channel width.</td></tr></table>				Option	Description	320MHz	320 MHz channel width.	240MHz	240 MHz channel width.	160MHz	160 MHz channel width.	80MHz	80 MHz channel width.	40MHz	40 MHz channel width.	20MHz	20 MHz channel width.
Option	Description																	
320MHz	320 MHz channel width.																	
240MHz	240 MHz channel width.																	
160MHz	160 MHz channel width.																	
80MHz	80 MHz channel width.																	
40MHz	40 MHz channel width.																	
20MHz	20 MHz channel width.																	
channel-bonding-ext	Channel bandwidth extension: 320 MHz-1 and 320 MHz-2 (default = 320 MHz-2).	option	-	320MHz-2														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>320MHz-1</td><td>320 MHz channel with channel center frequency numbered 31, 95, and 159.</td></tr><tr><td>320MHz-2</td><td>320 MHz channel with channel center frequency numbered 63, 127, and 191.</td></tr></table>				Option	Description	320MHz-1	320 MHz channel with channel center frequency numbered 31, 95, and 159.	320MHz-2	320 MHz channel with channel center frequency numbered 63, 127, and 191.								
Option	Description																	
320MHz-1	320 MHz channel with channel center frequency numbered 31, 95, and 159.																	
320MHz-2	320 MHz channel with channel center frequency numbered 63, 127, and 191.																	
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable measuring channel utilization.</td></tr><tr><td>disable</td><td>Disable measuring channel utilization.</td></tr></table>				Option	Description	enable	Enable measuring channel utilization.	disable	Disable measuring channel utilization.								
Option	Description																	
enable	Enable measuring channel utilization.																	
disable	Disable measuring channel utilization.																	
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).	option	-	enable														

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>			Enable support for both HT20 and HT40 on the same radio.
	<i>disable</i>			Disable support for both HT20 and HT40 on the same radio.
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is always using the most optimal channel (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>			Enable distributed automatic radio resource provisioning.
	<i>disable</i>			Disable distributed automatic radio resource provisioning.
drma	Enable/disable dynamic radio mode assignment (DRMA) (default = disable).	option	-	disable
	Option Description			
	<i>disable</i>			Disable dynamic radio mode assignment (DRMA).
	<i>enable</i>			Enable dynamic radio mode assignment (DRMA).
drma-sensitivity	Network Coverage Factor (NCF) percentage required to consider a radio as redundant (default = low).	option	-	low
	Option Description			
	<i>low</i>			Consider a radio as redundant when its NCF is 100%.
	<i>medium</i>			Consider a radio as redundant when its NCF is 95%.
	<i>high</i>			Consider a radio as redundant when its NCF is 90%.
dtim	Delivery Traffic Indication Map (DTIM) period (1 - 255, default = 1). Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	
frag-threshold	Maximum packet size that can be sent without fragmentation (800 - 2346 bytes, default = 2346).	integer	Minimum value: 800 Maximum value: 2346	
iperf-protocol	Iperf test protocol (default = "UDP").	option	-	udp

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>UDP.</td></tr><tr><td>tcp</td><td>TCP.</td></tr></table>	Option	Description	udp	UDP.	tcp	TCP.											
	Option	Description																
	udp	UDP.																
tcp	TCP.																	
iperf-server-port	Iperf service port number.	integer	Minimum value: 5001 0 Maximum value: 65535															
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 0 Maximum value: 4294967295															
max-distance	Maximum expected distance between the AP and clients (0 - 54000 m, default = 0).	integer	Minimum value: 0 0 Maximum value: 54000															
mimo-mode	Configure radio MIMO mode (default = default).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Default radio MIMO mode.</td></tr><tr><td>1x1</td><td>1x1 radio MIMO mode.</td></tr><tr><td>2x2</td><td>2x2 radio MIMO mode.</td></tr><tr><td>3x3</td><td>3x3 radio MIMO mode.</td></tr><tr><td>4x4</td><td>4x4 radio MIMO mode.</td></tr><tr><td>8x8</td><td>8x8 radio MIMO mode.</td></tr></table>	Option	Description	default	Default radio MIMO mode.	1x1	1x1 radio MIMO mode.	2x2	2x2 radio MIMO mode.	3x3	3x3 radio MIMO mode.	4x4	4x4 radio MIMO mode.	8x8	8x8 radio MIMO mode.			
	Option	Description																
	default	Default radio MIMO mode.																
	1x1	1x1 radio MIMO mode.																
	2x2	2x2 radio MIMO mode.																
	3x3	3x3 radio MIMO mode.																
	4x4	4x4 radio MIMO mode.																
8x8	8x8 radio MIMO mode.																	
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disabled</td><td>Radio 3 is disabled.</td></tr><tr><td>ap</td><td>Radio 3 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td>monitor</td><td>Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr></table>	Option	Description	disabled	Radio 3 is disabled.	ap	Radio 3 operates as an access point that allows WiFi clients to connect to your network.	monitor	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.									
	Option	Description																
	disabled	Radio 3 is disabled.																
ap	Radio 3 operates as an access point that allows WiFi clients to connect to your network.																	
monitor	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																	

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sniffer</i></td><td>Radio 3 operates as a sniffer capturing WiFi frames on air.</td></tr><tr><td><i>sam</i></td><td>Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.</td></tr></table>	Option	Description	<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.	<i>sam</i>	Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.																	
	Option	Description																						
	<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.																						
<i>sam</i>	Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.																							
optional-antenna	Optional antenna used on FAP (default = none).	option	-	none																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>custom</i></td><td>Customize optional antenna gain.</td></tr><tr><td><i>FANT-04ABGN-0606-O-N</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-1414-P-N</i></td><td>14 dBi(2.4GHz) and 14 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-8065-P-N</i></td><td>8 dBi(2.4GHz) and 6.5 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-0606-O-R</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-0606-P-R</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-10ACAX-1213-D-N</i></td><td>12 dBi(2.4GHz) and 13 dBi(5GHz).</td></tr><tr><td><i>FANT-08ABGN-1213-D-R</i></td><td>12 dBi(2.4GHz) and 13 dBi(5GHz).</td></tr></table>	Option	Description	<i>none</i>	None.	<i>custom</i>	Customize optional antenna gain.	<i>FANT-04ABGN-0606-O-N</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-04ABGN-1414-P-N</i>	14 dBi(2.4GHz) and 14 dBi(5GHz).	<i>FANT-04ABGN-8065-P-N</i>	8 dBi(2.4GHz) and 6.5 dBi(5GHz).	<i>FANT-04ABGN-0606-O-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-04ABGN-0606-P-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-10ACAX-1213-D-N</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).	<i>FANT-08ABGN-1213-D-R</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).			
	Option	Description																						
	<i>none</i>	None.																						
	<i>custom</i>	Customize optional antenna gain.																						
	<i>FANT-04ABGN-0606-O-N</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-04ABGN-1414-P-N</i>	14 dBi(2.4GHz) and 14 dBi(5GHz).																						
	<i>FANT-04ABGN-8065-P-N</i>	8 dBi(2.4GHz) and 6.5 dBi(5GHz).																						
	<i>FANT-04ABGN-0606-O-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-04ABGN-0606-P-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-10ACAX-1213-D-N</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).																						
<i>FANT-08ABGN-1213-D-R</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).																							
optional-antenna-gain	Optional antenna gain in dBi (0 to 20, default = 0).	string	Maximum length: 7	0																				
power-level	Radio EIRP power level as a percentage of the maximum EIRP power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100	100																				

Parameter	Description	Type	Size	Default												
power-mode	Set radio effective isotropic radiated power (EIRP) in dBm or by a percentage of the maximum EIRP (default = percentage). This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.									
Option	Description															
<i>dBm</i>	Set radio EIRP power in dBm.															
<i>percentage</i>	Set radio EIRP power by percentage.															
power-value	Radio EIRP power in dBm (1 - 33, default = 27).	integer	Minimum value: 27 1 Maximum value: 33													
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tim</i></td><td>TIM bit for client in power save mode.</td></tr><tr><td><i>ac-vo</i></td><td>Use AC VO priority to send out packets in the power save queue.</td></tr><tr><td><i>no-obss-scan</i></td><td>Do not put OBSS scan IE into beacon and probe response frames.</td></tr><tr><td><i>no-11b-rate</i></td><td>Do not send frame using 11b data rate.</td></tr><tr><td><i>client-rate-follow</i></td><td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td></tr></table>	Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.			
Option	Description															
<i>tim</i>	TIM bit for client in power save mode.															
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.															
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.															
<i>no-11b-rate</i>	Do not send frame using 11b data rate.															
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.															
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rtscts</i></td><td>Enable 802.11g protection RTS/CTS mode.</td></tr><tr><td><i>ctsonly</i></td><td>Enable 802.11g protection CTS only mode.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11g protection mode.</td></tr></table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.							
Option	Description															
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.															
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.															
<i>disable</i>	Disable 802.11g protection mode.															

Parameter	Description	Type	Size	Default								
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS (256 - 2346 bytes, default = 2346).	integer	Minimum value: 256 Maximum value: 2346	2346								
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00								
sam-ca-certificate	CA certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 79									
sam-captive-portal	Enable/disable Captive Portal Authentication (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Captive Portal Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable Captive Portal Authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable Captive Portal Authentication.	<i>disable</i>	Disable Captive Portal Authentication.		
Option	Description											
<i>enable</i>	Enable Captive Portal Authentication.											
<i>disable</i>	Disable Captive Portal Authentication.											
sam-client-certificate	Client certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35									
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64									
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64									
sam-cwp-password	Password for captive portal authentication.	password	Not Specified									
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64									
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255									
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35									
sam-eap-method	Select WPA2/WPA3-ENTERPRISE EAP Method (default = PEAP).	option	-	peap								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>both</i></td><td>EAP PEAP and TLS. (Not applicable in FIPS mode)</td></tr><tr><td><i>tls</i></td><td>EAP TLS.</td></tr><tr><td><i>peap</i></td><td>EAP PEAP. (Not applicable in FIPS mode)</td></tr></table>				Option	Description	<i>both</i>	EAP PEAP and TLS. (Not applicable in FIPS mode)	<i>tls</i>	EAP TLS.	<i>peap</i>	EAP PEAP. (Not applicable in FIPS mode)
Option	Description											
<i>both</i>	EAP PEAP and TLS. (Not applicable in FIPS mode)											
<i>tls</i>	EAP TLS.											
<i>peap</i>	EAP PEAP. (Not applicable in FIPS mode)											

Parameter	Description	Type	Size	Default												
sam-password	Passphrase for WiFi network connection.	password	Not Specified													
sam-private-key	Private key for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35													
sam-private-key-password	Password for private key file for WPA2/WPA3-ENTERPRISE.	password	Not Specified													
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0												
sam-security-type	Select WiFi network security type (default = "wpa-personal" for 2.4/5G radio, "wpa3-sae" for 6G radio).	option	-	wpa-personal												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>open</td><td>Open.</td></tr><tr><td>wpa-personal</td><td>WPA/WPA2 personal.</td></tr><tr><td>wpa-enterprise</td><td>WPA2/WPA3 enterprise.</td></tr><tr><td>wpa3-sae</td><td>WPA3 SAE.</td></tr><tr><td>owe</td><td>OWE.</td></tr></table>				Option	Description	open	Open.	wpa-personal	WPA/WPA2 personal.	wpa-enterprise	WPA2/WPA3 enterprise.	wpa3-sae	WPA3 SAE.	owe	OWE.
Option	Description															
open	Open.															
wpa-personal	WPA/WPA2 personal.															
wpa-enterprise	WPA2/WPA3 enterprise.															
wpa3-sae	WPA3 SAE.															
owe	OWE.															
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255													
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0												
sam-server-type	Select SAM server type (default = "IP").	option	-	ip												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ip</td><td>IPv4 address.</td></tr><tr><td>fqdn</td><td>Fully Qualified Domain Name address.</td></tr></table>				Option	Description	ip	IPv4 address.	fqdn	Fully Qualified Domain Name address.						
Option	Description															
ip	IPv4 address.															
fqdn	Fully Qualified Domain Name address.															
sam-ssid	SSID for WiFi network.	string	Maximum length: 32													
sam-test	Select SAM test type (default = "PING").	option	-	ping												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING test.</td></tr></table>				Option	Description	ping	PING test.								
Option	Description															
ping	PING test.															

Parameter	Description	Type	Size	Default
	Option Description			
	<i>iperf</i>	IPERF test.		
sam-username	Username for WiFi network connection.	string	Maximum length: 35	
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable
	Option Description			
	<i>enable</i>	Select the 400 ns short guard interval (Short GI).		
	<i>disable</i>	Select the 800 ns long guard interval (Long GI).		
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar
	Option Description			
	<i>disable</i>	Disable packet transmission optimization.		
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.		
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.		
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.		
	<i>send-bar</i>	Limit transmission of BAR frames.		
vap-all	Configure method for assigning SSIDs to this FortiAP (default = automatically assign tunnel SSIDs).	option	-	tunnel
	Option Description			
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35							
zero-wait-dfs	Enable/disable zero wait DFS on radio (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero wait DFS</td></tr><tr><td><i>disable</i></td><td>Disable zero wait DFS</td></tr></table>				Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS
Option	Description									
<i>enable</i>	Enable zero wait DFS									
<i>disable</i>	Disable zero wait DFS									

config radio-4

Parameter	Description	Type	Size	Default						
80211d	Enable/disable 802.11d countryie (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11d countryie.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11d countryie.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11d countryie.	<i>disable</i>	Disable 802.11d countryie.			
Option	Description									
<i>enable</i>	Enable 802.11d countryie.									
<i>disable</i>	Disable 802.11d countryie.									
80211mc	Enable/disable 802.11mc responder mode (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11mc responder mode.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11mc responder mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11mc responder mode.	<i>disable</i>	Disable 802.11mc responder mode.			
Option	Description									
<i>enable</i>	Enable 802.11mc responder mode.									
<i>disable</i>	Disable 802.11mc responder mode.									
airtime-fairness	Enable/disable airtime fairness (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td><i>disable</i></td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.			
Option	Description									
<i>enable</i>	Enable airtime fairness (ATF) support.									
<i>disable</i>	Disable airtime fairness (ATF) support.									
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients (default = enable).	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00
ap-sniffer-bufsize	Sniffer buffer size (1 - 32 MB, default = 16).	integer	Minimum value: 1 Maximum value: 32	16
ap-sniffer-chan	Channel on which to operate the sniffer (default = 6).	integer	Minimum value: 0 Maximum value: 4294967295	6
ap-sniffer-chan-width	Channel bandwidth for sniffer.	option	-	20MHz
	Option Description			
	<i>320MHz</i>	320 MHz channel width.		
	<i>240MHz</i>	240 MHz channel width.		
	<i>160MHz</i>	160 MHz channel width.		
	<i>80MHz</i>	80 MHz channel width.		
	<i>40MHz</i>	40 MHz channel width.		
	<i>20MHz</i>	20 MHz channel width.		
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable sniffer on WiFi control frame.		
	<i>disable</i>	Disable sniffer on WiFi control frame.		
ap-sniffer-data	Enable/disable sniffer on WiFi data frame (default = enable).	option	-	enable
	Option Description			
	<i>enable</i>	Enable sniffer on WiFi data frame		
	<i>disable</i>	Disable sniffer on WiFi data frame		

Parameter	Description	Type	Size	Default						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management other frame.									
<i>disable</i>	Disable sniffer on WiFi management other frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.			
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management probe frame.									
<i>disable</i>	Enable sniffer on WiFi management probe frame.									
arrp-profile	Distributed Automatic Radio Resource Provisioning (DARRP) profile name to assign to the radio.	string	Maximum length: 35							
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 17 0 Maximum value: 4294967295							
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									

Parameter	Description	Type	Size	Default																												
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 10 0 Maximum value: 4294967295																													
auto-power-target	Target of automatic transmit power adjustment in dBm (-95 to -20, default = -70).	string	Maximum length: 7	-70																												
band	WiFi band that Radio 4 operates on.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g.</td></tr><tr><td>802.11n-2G</td><td>802.11n (WiFi 4) at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n (WiFi 4) at 5GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac (WiFi 5) at 2.4GHz.</td></tr><tr><td>802.11ac-5G</td><td>802.11ac (WiFi 5) at 5GHz.</td></tr><tr><td>802.11ax-2G</td><td>802.11ax (WiFi 6) at 2.4GHz.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax (WiFi 6) at 5GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax (WiFi 6) at 6GHz.</td></tr><tr><td>802.11be-2G</td><td>802.11be (WiFi 7) at 2.4GHz.</td></tr><tr><td>802.11be-5G</td><td>802.11be (WiFi 7) at 5GHz.</td></tr><tr><td>802.11be-6G</td><td>802.11be (WiFi 7) at 6GHz.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g.	802.11n-2G	802.11n (WiFi 4) at 2.4GHz.	802.11n-5G	802.11n (WiFi 4) at 5GHz.	802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.	802.11ac-5G	802.11ac (WiFi 5) at 5GHz.	802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.	802.11ax-5G	802.11ax (WiFi 6) at 5GHz.	802.11ax-6G	802.11ax (WiFi 6) at 6GHz.	802.11be-2G	802.11be (WiFi 7) at 2.4GHz.	802.11be-5G	802.11be (WiFi 7) at 5GHz.	802.11be-6G	802.11be (WiFi 7) at 6GHz.			
Option	Description																															
802.11a	802.11a.																															
802.11b	802.11b.																															
802.11g	802.11g.																															
802.11n-2G	802.11n (WiFi 4) at 2.4GHz.																															
802.11n-5G	802.11n (WiFi 4) at 5GHz.																															
802.11ac-2G	802.11ac (WiFi 5) at 2.4GHz.																															
802.11ac-5G	802.11ac (WiFi 5) at 5GHz.																															
802.11ax-2G	802.11ax (WiFi 6) at 2.4GHz.																															
802.11ax-5G	802.11ax (WiFi 6) at 5GHz.																															
802.11ax-6G	802.11ax (WiFi 6) at 6GHz.																															
802.11be-2G	802.11be (WiFi 7) at 2.4GHz.																															
802.11be-5G	802.11be (WiFi 7) at 5GHz.																															
802.11be-6G	802.11be (WiFi 7) at 6GHz.																															
band-5g-type	WiFi 5G band type.	option	-	5g-full																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.																							
Option	Description																															
5g-full	Full 5G band.																															
5g-high	High 5G band.																															
5g-low	Low 5G band.																															

Parameter	Description	Type	Size	Default						
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 2000 1 Maximum value: 600000							
beacon-interval	Beacon interval. The time between beacon frames in milliseconds. Actual range of beacon interval depends on the AP platform type (default = 100).	integer	Minimum value: 100 0 Maximum value: 65535							
bss-color	BSS color value for this 11ax radio (0 - 63, disable = 0, default = 0).	integer	Minimum value: 0 0 Maximum value: 63							
bss-color-mode	BSS color mode for this 11ax radio (default = auto).	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically select BSS color value on AP.</td></tr><tr><td><i>static</i></td><td>Set BSS color value on this radio based on 'bss-color' CLI.</td></tr></table>	Option	Description	<i>auto</i>	Automatically select BSS color value on AP.	<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.			
Option	Description									
<i>auto</i>	Automatically select BSS color value on AP.									
<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.			
Option	Description									
<i>enable</i>	Enable WMM call admission control.									
<i>disable</i>	Disable WMM call admission control.									

Parameter	Description	Type	Size	Default														
call-capacity	Maximum number of Voice over WLAN (VoWLAN) phones supported by the radio (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60	10														
channel<chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3															
channel-bonding	Channel bandwidth: 320, 240, 160, 80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>320MHz</td><td>320 MHz channel width.</td></tr><tr><td>240MHz</td><td>240 MHz channel width.</td></tr><tr><td>160MHz</td><td>160 MHz channel width.</td></tr><tr><td>80MHz</td><td>80 MHz channel width.</td></tr><tr><td>40MHz</td><td>40 MHz channel width.</td></tr><tr><td>20MHz</td><td>20 MHz channel width.</td></tr></table>	Option	Description	320MHz	320 MHz channel width.	240MHz	240 MHz channel width.	160MHz	160 MHz channel width.	80MHz	80 MHz channel width.	40MHz	40 MHz channel width.	20MHz	20 MHz channel width.			
Option	Description																	
320MHz	320 MHz channel width.																	
240MHz	240 MHz channel width.																	
160MHz	160 MHz channel width.																	
80MHz	80 MHz channel width.																	
40MHz	40 MHz channel width.																	
20MHz	20 MHz channel width.																	
channel-bonding-ext	Channel bandwidth extension: 320 MHz-1 and 320 MHz-2 (default = 320 MHz-2).	option	-	320MHz-2														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>320MHz-1</td><td>320 MHz channel with channel center frequency numbered 31, 95, and 159.</td></tr><tr><td>320MHz-2</td><td>320 MHz channel with channel center frequency numbered 63, 127, and 191.</td></tr></table>	Option	Description	320MHz-1	320 MHz channel with channel center frequency numbered 31, 95, and 159.	320MHz-2	320 MHz channel with channel center frequency numbered 63, 127, and 191.											
Option	Description																	
320MHz-1	320 MHz channel with channel center frequency numbered 31, 95, and 159.																	
320MHz-2	320 MHz channel with channel center frequency numbered 63, 127, and 191.																	
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable measuring channel utilization.</td></tr><tr><td>disable</td><td>Disable measuring channel utilization.</td></tr></table>	Option	Description	enable	Enable measuring channel utilization.	disable	Disable measuring channel utilization.											
Option	Description																	
enable	Enable measuring channel utilization.																	
disable	Disable measuring channel utilization.																	
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).	option	-	enable														

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support for both HT20 and HT40 on the same radio.</td></tr><tr><td><i>disable</i></td><td>Disable support for both HT20 and HT40 on the same radio.</td></tr></table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.					
Option	Description											
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.											
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.											
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is always using the most optimal channel (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distributed automatic radio resource provisioning.</td></tr><tr><td><i>disable</i></td><td>Disable distributed automatic radio resource provisioning.</td></tr></table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.					
Option	Description											
<i>enable</i>	Enable distributed automatic radio resource provisioning.											
<i>disable</i>	Disable distributed automatic radio resource provisioning.											
drma	Enable/disable dynamic radio mode assignment (DRMA) (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dynamic radio mode assignment (DRMA).</td></tr><tr><td><i>enable</i></td><td>Enable dynamic radio mode assignment (DRMA).</td></tr></table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).					
Option	Description											
<i>disable</i>	Disable dynamic radio mode assignment (DRMA).											
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).											
drma-sensitivity	Network Coverage Factor (NCF) percentage required to consider a radio as redundant (default = low).	option	-	low								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Consider a radio as redundant when its NCF is 100%.</td></tr><tr><td><i>medium</i></td><td>Consider a radio as redundant when its NCF is 95%.</td></tr><tr><td><i>high</i></td><td>Consider a radio as redundant when its NCF is 90%.</td></tr></table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.			
Option	Description											
<i>low</i>	Consider a radio as redundant when its NCF is 100%.											
<i>medium</i>	Consider a radio as redundant when its NCF is 95%.											
<i>high</i>	Consider a radio as redundant when its NCF is 90%.											
dtim	Delivery Traffic Indication Map (DTIM) period (1 - 255, default = 1). Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255									
frag-threshold	Maximum packet size that can be sent without fragmentation (800 - 2346 bytes, default = 2346).	integer	Minimum value: 800 Maximum value: 2346	2346								
iperf-protocol	Iperf test protocol (default = "UDP").	option	-	udp								

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>UDP.</td></tr><tr><td>tcp</td><td>TCP.</td></tr></table>	Option	Description	udp	UDP.	tcp	TCP.											
	Option	Description																
	udp	UDP.																
tcp	TCP.																	
iperf-server-port	Iperf service port number.	integer	Minimum value: 5001 0 Maximum value: 65535															
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 0 Maximum value: 4294967295															
max-distance	Maximum expected distance between the AP and clients (0 - 54000 m, default = 0).	integer	Minimum value: 0 0 Maximum value: 54000															
mimo-mode	Configure radio MIMO mode (default = default).	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Default radio MIMO mode.</td></tr><tr><td>1x1</td><td>1x1 radio MIMO mode.</td></tr><tr><td>2x2</td><td>2x2 radio MIMO mode.</td></tr><tr><td>3x3</td><td>3x3 radio MIMO mode.</td></tr><tr><td>4x4</td><td>4x4 radio MIMO mode.</td></tr><tr><td>8x8</td><td>8x8 radio MIMO mode.</td></tr></table>	Option	Description	default	Default radio MIMO mode.	1x1	1x1 radio MIMO mode.	2x2	2x2 radio MIMO mode.	3x3	3x3 radio MIMO mode.	4x4	4x4 radio MIMO mode.	8x8	8x8 radio MIMO mode.			
	Option	Description																
	default	Default radio MIMO mode.																
	1x1	1x1 radio MIMO mode.																
	2x2	2x2 radio MIMO mode.																
	3x3	3x3 radio MIMO mode.																
	4x4	4x4 radio MIMO mode.																
8x8	8x8 radio MIMO mode.																	
mode	Mode of radio 4. Radio 4 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disabled</td><td>Radio 4 is disabled.</td></tr><tr><td>ap</td><td>Radio 4 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td>monitor</td><td>Radio 4 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr></table>	Option	Description	disabled	Radio 4 is disabled.	ap	Radio 4 operates as an access point that allows WiFi clients to connect to your network.	monitor	Radio 4 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.									
	Option	Description																
	disabled	Radio 4 is disabled.																
ap	Radio 4 operates as an access point that allows WiFi clients to connect to your network.																	
monitor	Radio 4 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																	

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sniffer</i></td><td>Radio 4 operates as a sniffer capturing WiFi frames on air.</td></tr><tr><td><i>sam</i></td><td>Radio 4 operates as a station that can connect to a neighboring AP for connectivity and health check.</td></tr></table>	Option	Description	<i>sniffer</i>	Radio 4 operates as a sniffer capturing WiFi frames on air.	<i>sam</i>	Radio 4 operates as a station that can connect to a neighboring AP for connectivity and health check.																	
	Option	Description																						
	<i>sniffer</i>	Radio 4 operates as a sniffer capturing WiFi frames on air.																						
<i>sam</i>	Radio 4 operates as a station that can connect to a neighboring AP for connectivity and health check.																							
optional-antenna	Optional antenna used on FAP (default = none).	option	-	none																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>custom</i></td><td>Customize optional antenna gain.</td></tr><tr><td><i>FANT-04ABGN-0606-O-N</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-1414-P-N</i></td><td>14 dBi(2.4GHz) and 14 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-8065-P-N</i></td><td>8 dBi(2.4GHz) and 6.5 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-0606-O-R</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-04ABGN-0606-P-R</i></td><td>6 dBi(2.4GHz) and 6 dBi(5GHz).</td></tr><tr><td><i>FANT-10ACAX-1213-D-N</i></td><td>12 dBi(2.4GHz) and 13 dBi(5GHz).</td></tr><tr><td><i>FANT-08ABGN-1213-D-R</i></td><td>12 dBi(2.4GHz) and 13 dBi(5GHz).</td></tr></table>	Option	Description	<i>none</i>	None.	<i>custom</i>	Customize optional antenna gain.	<i>FANT-04ABGN-0606-O-N</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-04ABGN-1414-P-N</i>	14 dBi(2.4GHz) and 14 dBi(5GHz).	<i>FANT-04ABGN-8065-P-N</i>	8 dBi(2.4GHz) and 6.5 dBi(5GHz).	<i>FANT-04ABGN-0606-O-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-04ABGN-0606-P-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).	<i>FANT-10ACAX-1213-D-N</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).	<i>FANT-08ABGN-1213-D-R</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).			
	Option	Description																						
	<i>none</i>	None.																						
	<i>custom</i>	Customize optional antenna gain.																						
	<i>FANT-04ABGN-0606-O-N</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-04ABGN-1414-P-N</i>	14 dBi(2.4GHz) and 14 dBi(5GHz).																						
	<i>FANT-04ABGN-8065-P-N</i>	8 dBi(2.4GHz) and 6.5 dBi(5GHz).																						
	<i>FANT-04ABGN-0606-O-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-04ABGN-0606-P-R</i>	6 dBi(2.4GHz) and 6 dBi(5GHz).																						
	<i>FANT-10ACAX-1213-D-N</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).																						
<i>FANT-08ABGN-1213-D-R</i>	12 dBi(2.4GHz) and 13 dBi(5GHz).																							
optional-antenna-gain	Optional antenna gain in dBi (0 to 20, default = 0).	string	Maximum length: 7	0																				
power-level	Radio EIRP power level as a percentage of the maximum EIRP power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100	100																				

Parameter	Description	Type	Size	Default												
power-mode	Set radio effective isotropic radiated power (EIRP) in dBm or by a percentage of the maximum EIRP (default = percentage). This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.									
Option	Description															
<i>dBm</i>	Set radio EIRP power in dBm.															
<i>percentage</i>	Set radio EIRP power by percentage.															
power-value	Radio EIRP power in dBm (1 - 33, default = 27).	integer	Minimum value: 27 1 Maximum value: 33													
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tim</i></td><td>TIM bit for client in power save mode.</td></tr><tr><td><i>ac-vo</i></td><td>Use AC VO priority to send out packets in the power save queue.</td></tr><tr><td><i>no-obss-scan</i></td><td>Do not put OBSS scan IE into beacon and probe response frames.</td></tr><tr><td><i>no-11b-rate</i></td><td>Do not send frame using 11b data rate.</td></tr><tr><td><i>client-rate-follow</i></td><td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td></tr></table>	Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.			
Option	Description															
<i>tim</i>	TIM bit for client in power save mode.															
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.															
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.															
<i>no-11b-rate</i>	Do not send frame using 11b data rate.															
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.															
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rtscts</i></td><td>Enable 802.11g protection RTS/CTS mode.</td></tr><tr><td><i>ctsonly</i></td><td>Enable 802.11g protection CTS only mode.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11g protection mode.</td></tr></table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.							
Option	Description															
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.															
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.															
<i>disable</i>	Disable 802.11g protection mode.															

Parameter	Description	Type	Size	Default								
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS (256 - 2346 bytes, default = 2346).	integer	Minimum value: 256 Maximum value: 2346	2346								
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00								
sam-ca-certificate	CA certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 79									
sam-captive-portal	Enable/disable Captive Portal Authentication (default = disable).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Captive Portal Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable Captive Portal Authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable Captive Portal Authentication.	<i>disable</i>	Disable Captive Portal Authentication.		
Option	Description											
<i>enable</i>	Enable Captive Portal Authentication.											
<i>disable</i>	Disable Captive Portal Authentication.											
sam-client-certificate	Client certificate for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35									
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64									
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64									
sam-cwp-password	Password for captive portal authentication.	password	Not Specified									
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64									
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255									
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35									
sam-eap-method	Select WPA2/WPA3-ENTERPRISE EAP Method (default = PEAP).	option	-	peap								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>both</i></td><td>EAP PEAP and TLS. (Not applicable in FIPS mode)</td></tr><tr><td><i>tls</i></td><td>EAP TLS.</td></tr><tr><td><i>peap</i></td><td>EAP PEAP. (Not applicable in FIPS mode)</td></tr></table>				Option	Description	<i>both</i>	EAP PEAP and TLS. (Not applicable in FIPS mode)	<i>tls</i>	EAP TLS.	<i>peap</i>	EAP PEAP. (Not applicable in FIPS mode)
Option	Description											
<i>both</i>	EAP PEAP and TLS. (Not applicable in FIPS mode)											
<i>tls</i>	EAP TLS.											
<i>peap</i>	EAP PEAP. (Not applicable in FIPS mode)											

Parameter	Description	Type	Size	Default												
sam-password	Passphrase for WiFi network connection.	password	Not Specified													
sam-private-key	Private key for WPA2/WPA3-ENTERPRISE.	string	Maximum length: 35													
sam-private-key-password	Password for private key file for WPA2/WPA3-ENTERPRISE.	password	Not Specified													
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0												
sam-security-type	Select WiFi network security type (default = "wpa-personal" for 2.4/5G radio, "wpa3-sae" for 6G radio).	option	-	wpa-personal												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>open</td><td>Open.</td></tr><tr><td>wpa-personal</td><td>WPA/WPA2 personal.</td></tr><tr><td>wpa-enterprise</td><td>WPA2/WPA3 enterprise.</td></tr><tr><td>wpa3-sae</td><td>WPA3 SAE.</td></tr><tr><td>owe</td><td>OWE.</td></tr></table>				Option	Description	open	Open.	wpa-personal	WPA/WPA2 personal.	wpa-enterprise	WPA2/WPA3 enterprise.	wpa3-sae	WPA3 SAE.	owe	OWE.
Option	Description															
open	Open.															
wpa-personal	WPA/WPA2 personal.															
wpa-enterprise	WPA2/WPA3 enterprise.															
wpa3-sae	WPA3 SAE.															
owe	OWE.															
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255													
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0												
sam-server-type	Select SAM server type (default = "IP").	option	-	ip												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ip</td><td>IPv4 address.</td></tr><tr><td>fqdn</td><td>Fully Qualified Domain Name address.</td></tr></table>				Option	Description	ip	IPv4 address.	fqdn	Fully Qualified Domain Name address.						
Option	Description															
ip	IPv4 address.															
fqdn	Fully Qualified Domain Name address.															
sam-ssid	SSID for WiFi network.	string	Maximum length: 32													
sam-test	Select SAM test type (default = "PING").	option	-	ping												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING test.</td></tr></table>				Option	Description	ping	PING test.								
Option	Description															
ping	PING test.															

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>iperf</i></td><td>IPERF test.</td></tr></table>		Option	Description	<i>iperf</i>	IPERF test.										
	Option	Description														
<i>iperf</i>	IPERF test.															
sam-username	Username for WiFi network connection.	string	Maximum length: 35													
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td><i>disable</i></td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>		Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).								
	Option	Description														
	<i>enable</i>	Select the 400 ns short guard interval (Short GI).														
<i>disable</i>	Select the 800 ns long guard interval (Long GI).															
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet transmission optimization.</td></tr><tr><td><i>power-save</i></td><td>Tag client as operating in power save mode if excessive transmit retries occur.</td></tr><tr><td><i>aggr-limit</i></td><td>Set aggregation limit to a lower value when data rate is low.</td></tr><tr><td><i>retry-limit</i></td><td>Set software retry limit to a lower value when data rate is low.</td></tr><tr><td><i>send-bar</i></td><td>Limit transmission of BAR frames.</td></tr></table>		Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.		
	Option	Description														
	<i>disable</i>	Disable packet transmission optimization.														
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.														
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.														
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.														
<i>send-bar</i>	Limit transmission of BAR frames.															
vap-all	Configure method for assigning SSIDs to this FortiAP (default = automatically assign tunnel SSIDs).	option	-	tunnel												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>		Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.						
	Option	Description														
	<i>tunnel</i>	Automatically select tunnel SSIDs.														
	<i>bridge</i>	Automatically select local-bridging SSIDs.														
<i>manual</i>	Manually select SSIDs.															
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35													

Parameter	Description	Type	Size	Default
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35	
zero-wait-dfs	Enable/disable zero wait DFS on radio (default = enable).	option	-	enable
	Option	Description		
	enable	Enable zero wait DFS		
	disable	Disable zero wait DFS		

config split-tunneling-acl

Parameter	Description	Type	Size	Default
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

ztna

This section includes syntax for the following commands:

- [config ztna reverse-connector on page 2662](#)
- [config ztna traffic-forward-proxy on page 2663](#)
- [config ztna web-portal-bookmark on page 2668](#)
- [config ztna web-portal on page 2664](#)
- [config ztna web-proxy on page 2675](#)

config ztna reverse-connector

Configure ZTNA Reverse-Connector.

```
config ztna reverse-connector
  Description: Configure ZTNA Reverse-Connector.
  edit <name>
    set address {string}
    set certificate {string}
    set health-check-interval {integer}
    set port {integer}
    set ssl-max-version [tls-1.1|tls-1.2|...]
    set status [enable|disable]
    set trusted-server-ca {string}
  next
end
```

config ztna reverse-connector

Parameter	Description	Type	Size	Default
address	Connector service edge adress(IP or FQDN).	string	Maximum length: 255	
certificate	The name of the certificate to use for SSL handshake.	string	Maximum length: 35	
health-check-interval	Health check interval in seconds (0 - 600, default = 60, 0 = disable).	integer	Minimum value: 0 Maximum value: 600	60

Parameter	Description	Type	Size	Default								
name	Reverse-Connector name	string	Maximum length: 35									
port	Port number that traffic uses to connect to connector service edge(0 - 65535;).	integer	Minimum value: 0 Maximum value: 65535	0								
ssl-max-version	Highest TLS version acceptable from a server.	option	-	tls-1.3								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>				Option	Description	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.
Option	Description											
tls-1.1	TLS 1.1.											
tls-1.2	TLS 1.2.											
tls-1.3	TLS 1.3.											
status	Reverse-Connector status.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable the reverse-connector.</td></tr><tr><td>disable</td><td>Disable the reverse-connector.</td></tr></table>				Option	Description	enable	Enable the reverse-connector.	disable	Disable the reverse-connector.		
Option	Description											
enable	Enable the reverse-connector.											
disable	Disable the reverse-connector.											
trusted-server-ca	Trusted Server CA certificate used by SSL connection.	string	Maximum length: 79									

config ztna traffic-forward-proxy

Configure ZTNA traffic forward proxy.

```

config ztna traffic-forward-proxy
  Description: Configure ZTNA traffic forward proxy.
  edit <name>
    set auth-portal [disable|enable]
    set auth-virtual-host {string}
    set decrypted-traffic-mirror {string}
    set host {string}
    set log-blocked-traffic [disable|enable]
    set vip {string}
    set vip6 {string}
  next
end

```

config ztna traffic-forward-proxy

Parameter	Description	Type	Size	Default
auth-portal	Enable/disable authentication portal.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable authentication portal.		
	<i>enable</i>	Enable authentication portal.		
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79	
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35	
host	Virtual or real host name.	string	Maximum length: 79	
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	enable
	Option	Description		
	<i>disable</i>	Do not log all traffic denied by this ZTNA web-proxy.		
	<i>enable</i>	Log all traffic denied by this ZTNA web-proxy.		
name	ZTNA proxy name.	string	Maximum length: 79	
vip	Virtual IP name.	string	Maximum length: 79	
vip6	Virtual IPv6 name.	string	Maximum length: 79	

config ztna web-portal

Configure ztna web-portal.

```
config ztna web-portal
  Description: Configure ztna web-portal.
  edit <name>
    set auth-portal [disable|enable]
    set auth-rule {string}
    set auth-virtual-host {string}
    set clipboard [enable|disable]
    set cookie-age {integer}
    set customize-forticlient-download-url [enable|disable]
```



```

set decrypted-traffic-mirror {string}
set default-window-height {integer}
set default-window-width {integer}
set display-bookmark [enable|disable]
set display-history [enable|disable]
set display-status [enable|disable]
set focus-bookmark [enable|disable]
set forticlient-download [enable|disable]
set forticlient-download-method [direct|ssl-vpn]
set heading {string}
set host {string}
set log-blocked-traffic [disable|enable]
set macos-forticlient-download-url {var-string}
set policy-auth-sso [enable|disable]
set theme [jade|neutrino|...]
set vip {string}
set vip6 {string}
set windows-forticlient-download-url {var-string}
next
end

```

config ztna web-portal

Parameter	Description	Type	Size	Default						
auth-portal	Enable/disable authentication portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable authentication portal.</td></tr><tr><td>enable</td><td>Enable authentication portal.</td></tr></table>	Option	Description	disable	Disable authentication portal.	enable	Enable authentication portal.			
	Option	Description								
	disable	Disable authentication portal.								
enable	Enable authentication portal.									
auth-rule	Authentication Rule.	string	Maximum length: 35							
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79							
clipboard	Enable to support RDP/VPC clipboard functionality.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable support of RDP/VNC clipboard.</td></tr><tr><td>disable</td><td>Disable support of RDP/VNC clipboard.</td></tr></table>	Option	Description	enable	Enable support of RDP/VNC clipboard.	disable	Disable support of RDP/VNC clipboard.			
	Option	Description								
	enable	Enable support of RDP/VNC clipboard.								
disable	Disable support of RDP/VNC clipboard.									
cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						

Parameter	Description	Type	Size	Default						
customize-forticlient-download-url	Enable support of customized download URL for FortiClient.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
default-window-height	Screen height (range from 0 - 65535, default = 768).	integer	Minimum value: 0 Maximum value: 65535	768						
default-window-width	Screen width (range from 0 - 65535, default = 1024).	integer	Minimum value: 0 Maximum value: 65535	1024						
display-bookmark	Enable to display the web portal bookmark widget.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
display-history	Enable to display the web portal user login history widget.	option	-	disable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
display-status	Enable to display the web portal status widget.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									

Parameter	Description	Type	Size	Default
focus-bookmark	Enable to prioritize the placement of the bookmark section over the quick-connection section in the ztna web-portal.	option	-	disable
	Option			
	<i>enable</i>			
	<i>disable</i>			
forticlient-download	Enable/disable download option for FortiClient.	option	-	enable
	Option			
	<i>enable</i>			
	<i>disable</i>			
forticlient-download-method	FortiClient download method.	option	-	direct
	Option			
	<i>direct</i>			
	<i>ssl-vpn</i>			
heading	Web portal heading message.	string	Maximum length: 31	ZTNA Portal
host	Virtual or real host name.	string	Maximum length: 79	
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	enable
	Option			
	<i>disable</i>			
	<i>enable</i>			
macos-forticlient-download-url	Download URL for Mac FortiClient.	var-string	Maximum length: 1023	
name	ZTNA proxy name.	string	Maximum length: 79	
policy-auth-sso	Enable policy sso authentication.	option	-	enable

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																			
	Option	Description																								
	<i>enable</i>	Enable setting.																								
<i>disable</i>	Disable setting.																									
theme	Web portal color scheme.	option	-	security-fabric																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>jade</i></td><td>Jade theme.</td></tr><tr><td><i>neutrino</i></td><td>Neutrino theme.</td></tr><tr><td><i>mariner</i></td><td>Mariner theme.</td></tr><tr><td><i>graphite</i></td><td>Graphite theme.</td></tr><tr><td><i>melongene</i></td><td>Melongene theme.</td></tr><tr><td><i>jet-stream</i></td><td>Jet Stream theme.</td></tr><tr><td><i>security-fabric</i></td><td>Security Fabric theme.</td></tr><tr><td><i>dark-matter</i></td><td>Dark Matter theme.</td></tr><tr><td><i>onyx</i></td><td>Onyx theme.</td></tr><tr><td><i>eclipse</i></td><td>Eclipse theme.</td></tr></table>	Option	Description	<i>jade</i>	Jade theme.	<i>neutrino</i>	Neutrino theme.	<i>mariner</i>	Mariner theme.	<i>graphite</i>	Graphite theme.	<i>melongene</i>	Melongene theme.	<i>jet-stream</i>	Jet Stream theme.	<i>security-fabric</i>	Security Fabric theme.	<i>dark-matter</i>	Dark Matter theme.	<i>onyx</i>	Onyx theme.	<i>eclipse</i>	Eclipse theme.			
	Option	Description																								
	<i>jade</i>	Jade theme.																								
	<i>neutrino</i>	Neutrino theme.																								
	<i>mariner</i>	Mariner theme.																								
	<i>graphite</i>	Graphite theme.																								
	<i>melongene</i>	Melongene theme.																								
	<i>jet-stream</i>	Jet Stream theme.																								
	<i>security-fabric</i>	Security Fabric theme.																								
	<i>dark-matter</i>	Dark Matter theme.																								
<i>onyx</i>	Onyx theme.																									
<i>eclipse</i>	Eclipse theme.																									
vip	Virtual IP name.	string	Maximum length: 79																							
vip6	Virtual IPv6 name.	string	Maximum length: 79																							
windows-forticlient-download-url	Download URL for Windows FortiClient.	var-string	Maximum length: 1023																							

** Values may differ between models.

config ztna web-portal-bookmark

Configure ztna web-portal bookmark.

```

config ztna web-portal-bookmark
  Description: Configure ztna web-portal bookmark.
  edit <name>
    config bookmarks
      Description: Bookmark table.
      edit <name>

```

```

        set apptype [ftp|rdp|...]
        set color-depth [32|16|...]
        set description {var-string}
        set domain {var-string}
        set folder {var-string}
        set height {integer}
        set host {var-string}
        set keyboard-layout [ar-101|ar-102|...]
        set load-balancing-info {var-string}
        set logon-password {password}
        set logon-user {var-string}
        set port {integer}
        set preconnection-blob {var-string}
        set preconnection-id {integer}
        set restricted-admin [enable|disable]
        set security [any|rdp|...]
        set send-preconnection-id [enable|disable]
        set sso [disable|enable]
        set url {var-string}
        set vnc-keyboard-layout [default|da|...]
        set width {integer}
    next
end
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
next
end

```

config ztna web-portal-bookmark

Parameter	Description	Type	Size	Default
groups <name>	User groups. Group name.	string	Maximum length: 79	
name	Bookmark name.	string	Maximum length: 35	
users <name>	User name. User name.	string	Maximum length: 79	

config bookmarks

Parameter	Description	Type	Size	Default
apptype	Application type.	option	-	web

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>rdp</td><td>RDP.</td></tr><tr><td>sftp</td><td>SFTP.</td></tr><tr><td>smb</td><td>SMB/CIFS.</td></tr><tr><td>ssh</td><td>SSH.</td></tr><tr><td>telnet</td><td>Telnet.</td></tr><tr><td>vnc</td><td>VNC.</td></tr><tr><td>web</td><td>HTTP/HTTPS.</td></tr></table>	Option	Description	ftp	FTP.	rdp	RDP.	sftp	SFTP.	smb	SMB/CIFS.	ssh	SSH.	telnet	Telnet.	vnc	VNC.	web	HTTP/HTTPS.			
	Option	Description																				
	ftp	FTP.																				
	rdp	RDP.																				
	sftp	SFTP.																				
	smb	SMB/CIFS.																				
	ssh	SSH.																				
	telnet	Telnet.																				
	vnc	VNC.																				
web	HTTP/HTTPS.																					
color-depth	Color depth per pixel.	option	-	16																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>32</td><td>32bits per pixel.</td></tr><tr><td>16</td><td>16bits per pixel.</td></tr><tr><td>8</td><td>8bits per pixel.</td></tr></table>	Option	Description	32	32bits per pixel.	16	16bits per pixel.	8	8bits per pixel.													
	Option	Description																				
	32	32bits per pixel.																				
	16	16bits per pixel.																				
8	8bits per pixel.																					
description	Description.	var-string	Maximum length: 128																			
domain	Login domain.	var-string	Maximum length: 128																			
folder	Network shared file folder parameter.	var-string	Maximum length: 128																			
height	Screen height (range from 0 - 65535, default = 0).	integer	Minimum value: 0 0 Maximum value: 65535																			
host	Host name/IP parameter.	var-string	Maximum length: 128																			
keyboard-layout	Keyboard layout.	option	-	en-us																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ar-101</td><td>Arabic (101).</td></tr><tr><td>ar-102</td><td>Arabic (102).</td></tr><tr><td>ar-102-azerty</td><td>Arabic (102) AZERTY.</td></tr><tr><td>can-mul</td><td>Canadian Multilingual Standard.</td></tr></table>	Option	Description	ar-101	Arabic (101).	ar-102	Arabic (102).	ar-102-azerty	Arabic (102) AZERTY.	can-mul	Canadian Multilingual Standard.											
	Option	Description																				
	ar-101	Arabic (101).																				
	ar-102	Arabic (102).																				
	ar-102-azerty	Arabic (102) AZERTY.																				
can-mul	Canadian Multilingual Standard.																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>cz</i>	Czech.		
	<i>cz-qwerty</i>	Czech (QWERTY).		
	<i>cz-pr</i>	Czech Programmers.		
	<i>da</i>	Danish.		
	<i>nl</i>	Dutch.		
	<i>de</i>	German.		
	<i>de-ch</i>	German, Switzerland.		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finnish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-apple</i>	French, Apple.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgium.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ja-106</i>	Japanese 106/109 key.		
	<i>ko</i>	Korean.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>la-am</i>	Latin American.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		
	<i>lt-std</i>	Lithuanian Standard.		
	<i>lav-std</i>	Latvian (Standard).		
	<i>lav-leg</i>	Latvian (Legacy).		
	<i>mk</i>	Macedonian (FYROM).		
	<i>mk-std</i>	Macedonia (FYROM) - Standard.		
	<i>no</i>	Norwegian.		
	<i>no-sami</i>	Norwegian with Sami.		
	<i>pol-214</i>	Polish (214).		
	<i>pol-pr</i>	Polish (Programmers).		
	<i>pt</i>	Portuguese.		
	<i>pt-br</i>	Portuguese (Brazilian ABNT).		
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).		
	<i>ru</i>	Russian.		
	<i>ru-mne</i>	Russian - Mnemonic.		
	<i>ru-t</i>	Russian (Typewriter).		
	<i>sl</i>	Slovenian.		
	<i>sv</i>	Swedish.		
	<i>sv-sami</i>	Swedish with Sami.		
	<i>tuk</i>	Turkmen.		
	<i>tur-f</i>	Turkish F.		
	<i>tur-q</i>	Turkish Q.		
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.		
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.		
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).		
	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.		
	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.		

Parameter	Description	Type	Size	Default										
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511											
logon-password	Logon password.	password	Not Specified											
logon-user	Logon user.	var-string	Maximum length: 35											
name	Bookmark name.	string	Maximum length: 35											
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535											
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511											
preconnection-id	The numeric ID of the RDP source (0-4294967295).	integer	Minimum value: 0 Maximum value: 4294967295											
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable restricted admin mode for RDP.</td></tr><tr><td>disable</td><td>Disable restricted admin mode for RDP.</td></tr></table>				Option	Description	enable	Enable restricted admin mode for RDP.	disable	Disable restricted admin mode for RDP.				
Option	Description													
enable	Enable restricted admin mode for RDP.													
disable	Disable restricted admin mode for RDP.													
security	Security mode for RDP connection (default = any).	option	-	any										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>any</td><td>Allow the server to choose the type of security.</td></tr><tr><td>rdp</td><td>Standard RDP encryption.</td></tr><tr><td>nla</td><td>Network Level Authentication.</td></tr><tr><td>tls</td><td>TLS encryption.</td></tr></table>				Option	Description	any	Allow the server to choose the type of security.	rdp	Standard RDP encryption.	nla	Network Level Authentication.	tls	TLS encryption.
Option	Description													
any	Allow the server to choose the type of security.													
rdp	Standard RDP encryption.													
nla	Network Level Authentication.													
tls	TLS encryption.													
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending of preconnection ID.</td></tr><tr><td>disable</td><td>Disable sending of preconnection ID.</td></tr></table>				Option	Description	enable	Enable sending of preconnection ID.	disable	Disable sending of preconnection ID.				
Option	Description													
enable	Enable sending of preconnection ID.													
disable	Disable sending of preconnection ID.													

Parameter	Description	Type	Size	Default																																										
sso	Single sign-on.	option	-	disable																																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SSO.</td></tr><tr><td>enable</td><td>Enable SSO.</td></tr></table>				Option	Description	disable	Disable SSO.	enable	Enable SSO.																																				
	Option	Description																																												
	disable	Disable SSO.																																												
enable	Enable SSO.																																													
url	URL parameter.	var-string	Maximum length: 128																																											
vnc-keyboard-layout	Keyboard layout.	option	-	default																																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Default.</td></tr><tr><td>da</td><td>Danish.</td></tr><tr><td>nl</td><td>Dutch.</td></tr><tr><td>en-uk</td><td>English, United Kingdom.</td></tr><tr><td>en-uk-ext</td><td>English, United Kingdom Extended.</td></tr><tr><td>fi</td><td>Finnish.</td></tr><tr><td>fr</td><td>French.</td></tr><tr><td>fr-be</td><td>French, Belgium.</td></tr><tr><td>fr-ca-mul</td><td>French, Canadian Multilingual Std.</td></tr><tr><td>de</td><td>German.</td></tr><tr><td>de-ch</td><td>German, Switzerland.</td></tr><tr><td>it</td><td>Italian.</td></tr><tr><td>it-142</td><td>Italian (142).</td></tr><tr><td>pt</td><td>Portuguese.</td></tr><tr><td>pt-br-abnt2</td><td>Portuguese (Brazilian ABNT2).</td></tr><tr><td>no</td><td>Norwegian.</td></tr><tr><td>gd</td><td>Scottish Gaelic.</td></tr><tr><td>es</td><td>Spanish.</td></tr><tr><td>sv</td><td>Swedish.</td></tr><tr><td>us-intl</td><td>United States-International.</td></tr></table>				Option	Description	default	Default.	da	Danish.	nl	Dutch.	en-uk	English, United Kingdom.	en-uk-ext	English, United Kingdom Extended.	fi	Finnish.	fr	French.	fr-be	French, Belgium.	fr-ca-mul	French, Canadian Multilingual Std.	de	German.	de-ch	German, Switzerland.	it	Italian.	it-142	Italian (142).	pt	Portuguese.	pt-br-abnt2	Portuguese (Brazilian ABNT2).	no	Norwegian.	gd	Scottish Gaelic.	es	Spanish.	sv	Swedish.	us-intl	United States-International.
	Option	Description																																												
	default	Default.																																												
	da	Danish.																																												
	nl	Dutch.																																												
	en-uk	English, United Kingdom.																																												
	en-uk-ext	English, United Kingdom Extended.																																												
	fi	Finnish.																																												
	fr	French.																																												
	fr-be	French, Belgium.																																												
	fr-ca-mul	French, Canadian Multilingual Std.																																												
	de	German.																																												
	de-ch	German, Switzerland.																																												
	it	Italian.																																												
	it-142	Italian (142).																																												
	pt	Portuguese.																																												
	pt-br-abnt2	Portuguese (Brazilian ABNT2).																																												
	no	Norwegian.																																												
	gd	Scottish Gaelic.																																												
	es	Spanish.																																												
sv	Swedish.																																													
us-intl	United States-International.																																													
width	Screen width (range from 0 - 65535, default = 0).	integer	Minimum value: 0 0 Maximum value: 65535																																											

config ztna web-proxy

Configure ZTNA web-proxy.

```
config ztna web-proxy
  Description: Configure ZTNA web-proxy.
  edit <name>
    config api-gateway
      Description: Set IPv4 API Gateway.
      edit <id>
        set h2-support [enable|disable]
        set h3-support [enable|disable]
        set http-cookie-age {integer}
        set http-cookie-domain {string}
        set http-cookie-domain-from-host [disable|enable]
        set http-cookie-generation {integer}
        set http-cookie-path {string}
        set http-cookie-share [disable|same-ip]
        set https-cookie-secure [disable|enable]
        set ldb-method [static|round-robin|...]
        set persistence [none|http-cookie]
      config quic
        Description: QUIC setting.
        set ack-delay-exponent {integer}
        set active-connection-id-limit {integer}
        set active-migration [enable|disable]
        set grease-quic-bit [enable|disable]
        set max-ack-delay {integer}
        set max-datagram-frame-size {integer}
        set max-idle-timeout {integer}
        set max-udp-payload-size {integer}
      end
    config realservers
      Description: Select the real servers that this Access Proxy will distribute
      traffic to.
      edit <id>
        set addr-type [ip|fqdn]
        set address {string}
        set health-check [disable|enable]
        set health-check-proto [ping|http|...]
        set holddown-interval [enable|disable]
        set http-host {string}
        set ip {ipv4-address-any}
        set port {integer}
        set status [active|standby|...]
        set translate-host [enable|disable]
        set verify-cert [enable|disable]
        set weight {integer}
      next
    end
  set service [http|https]
```

```

    set ssl-algorithm [high|medium|...]
    config ssl-cipher-suites
        Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
        edit <priority>
            set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
            set versions {option1}, {option2}, ...
        next
    end
    set ssl-dh-bits [768|1024|...]
    set ssl-max-version [tls-1.0|tls-1.1|...]
    set ssl-min-version [tls-1.0|tls-1.1|...]
    set ssl-renegotiation [enable|disable]
    set url-map {string}
    set url-map-type [sub-string|wildcard|...]
next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set h2-support [enable|disable]
        set h3-support [enable|disable]
        set http-cookie-age {integer}
        set http-cookie-domain {string}
        set http-cookie-domain-from-host [disable|enable]
        set http-cookie-generation {integer}
        set http-cookie-path {string}
        set http-cookie-share [disable|same-ip]
        set https-cookie-secure [disable|enable]
        set ldb-method [static|round-robin|...]
        set persistence [none|http-cookie]
    config quic
        Description: QUIC setting.
        set ack-delay-exponent {integer}
        set active-connection-id-limit {integer}
        set active-migration [enable|disable]
        set grease-quic-bit [enable|disable]
        set max-ack-delay {integer}
        set max-datagram-frame-size {integer}
        set max-idle-timeout {integer}
        set max-udp-payload-size {integer}
    end
    config realservers
        Description: Select the real servers that this Access Proxy will distribute
traffic to.
        edit <id>
            set addr-type [ip|fqdn]
            set address {string}
            set health-check [disable|enable]
            set health-check-proto [ping|http|...]
            set holddown-interval [enable|disable]
            set http-host {string}
            set ip {ipv6-address}

```

```

        set port {integer}
        set status [active|standby|...]
        set translate-host [enable|disable]
        set verify-cert [enable|disable]
        set weight {integer}
    next
end
set service [http|https]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-dh-bits [768|1024|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-min-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
set url-map {string}
set url-map-type [sub-string|wildcard|...]
next
end
set auth-portal [disable|enable]
set auth-virtual-host {string}
set decrypted-traffic-mirror {string}
set host {string}
set log-blocked-traffic [disable|enable]
set svr-pool-multiplex [enable|disable]
set svr-pool-server-max-concurrent-request {integer}
set svr-pool-server-max-request {integer}
set svr-pool-ttl {integer}
set vip {string}
set vip6 {string}
next
end

```

config ztna web-proxy

Parameter	Description	Type	Size	Default
auth-portal	Enable/disable authentication portal.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable authentication portal.		
	<i>enable</i>	Enable authentication portal.		

Parameter	Description	Type	Size	Default						
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79							
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
host	Virtual or real host name.	string	Maximum length: 79							
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not log all traffic denied by this ZTNA web-proxy.</td></tr><tr><td>enable</td><td>Log all traffic denied by this ZTNA web-proxy.</td></tr></table>				Option	Description	disable	Do not log all traffic denied by this ZTNA web-proxy.	enable	Log all traffic denied by this ZTNA web-proxy.
Option	Description									
disable	Do not log all traffic denied by this ZTNA web-proxy.									
enable	Log all traffic denied by this ZTNA web-proxy.									
name	ZTNA proxy name.	string	Maximum length: 79							
svr-pool-multiplex	Enable/disable server pool multiplexing. Share connected server in HTTP and HTTPS api-gateways.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable server pool multiplexing. Share connected server.</td></tr><tr><td>disable</td><td>Disable server pool multiplexing. Do not share connected server.</td></tr></table>				Option	Description	enable	Enable server pool multiplexing. Share connected server.	disable	Disable server pool multiplexing. Do not share connected server.
Option	Description									
enable	Enable server pool multiplexing. Share connected server.									
disable	Disable server pool multiplexing. Do not share connected server.									
svr-pool-server-max-concurrent-request	Maximum number of concurrent requests that servers in the server pool could handle (default = unlimited).	integer	Minimum value: 0 Maximum value: 2147483647	0						
svr-pool-server-max-request	Maximum number of requests that servers in the server pool handle before disconnecting (default = unlimited).	integer	Minimum value: 0 Maximum value: 2147483647	0						
svr-pool-ttl	Time-to-live in the server pool for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15						
vip	Virtual IP name.	string	Maximum length: 79							
vip6	Virtual IPv6 name.	string	Maximum length: 79							

config api-gateway

Parameter	Description	Type	Size	Default
h2-support	HTTP2 support, default=Enable.	option	-	enable
	Option Description			
	<i>enable</i>	Enable HTTP2 support.		
	<i>disable</i>	Disable HTTP2 support.		
h3-support	HTTP3/QUIC support, default=Disable.	option	-	disable
	Option Description			
	<i>enable</i>	Enable HTTP3/QUIC support.		
	<i>disable</i>	Disable HTTP3/QUIC support.		
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	Option Description			
	<i>disable</i>	Disable use of HTTP cookie domain from the host field in HTTP (use http-cooke-domain setting).		
	<i>enable</i>	Enable use of HTTP cookie domain from the host field in HTTP.		
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35	
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	Option Description			
	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.		
	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with the same IP.		

Parameter	Description	Type	Size	Default												
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark the cookie as secure. Allows sharing the cookie between HTTP and HTTPS connections.</td></tr><tr><td><i>enable</i></td><td>Mark the inserted cookie as secure. The cookie can only be used for HTTPS connections.</td></tr></table>	Option	Description	<i>disable</i>	Do not mark the cookie as secure. Allows sharing the cookie between HTTP and HTTPS connections.	<i>enable</i>	Mark the inserted cookie as secure. The cookie can only be used for HTTPS connections.									
Option	Description															
<i>disable</i>	Do not mark the cookie as secure. Allows sharing the cookie between HTTP and HTTPS connections.															
<i>enable</i>	Mark the inserted cookie as secure. The cookie can only be used for HTTPS connections.															
id	API Gateway ID.	integer	Minimum value: 0 0 Maximum value: 4294967295													
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute to servers based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute to servers based on round-robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute to servers based on weight.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to servers based on the host field in HTTP header.</td></tr></table>	Option	Description	<i>static</i>	Distribute to servers based on source IP.	<i>round-robin</i>	Distribute to servers based on round-robin order.	<i>weighted</i>	Distribute to servers based on weight.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to servers based on the host field in HTTP header.			
Option	Description															
<i>static</i>	Distribute to servers based on source IP.															
<i>round-robin</i>	Distribute to servers based on round-robin order.															
<i>weighted</i>	Distribute to servers based on weight.															
<i>first-alive</i>	Distribute to the first server that is alive.															
<i>http-host</i>	Distribute to servers based on the host field in HTTP header.															
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.									
Option	Description															
<i>none</i>	None.															
<i>http-cookie</i>	HTTP cookie.															
service	Service.	option	-	https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.									
Option	Description															
<i>http</i>	HTTP.															
<i>https</i>	HTTPS.															
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high												

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.									
	Option	Description																
	<i>high</i>	High encryption. Allow only AES and ChaCha.																
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.			
	Option	Description																
	768	768-bit Diffie-Hellman prime.																
	1024	1024-bit Diffie-Hellman prime.																
	1536	1536-bit Diffie-Hellman prime.																
	2048	2048-bit Diffie-Hellman prime.																
	3072	3072-bit Diffie-Hellman prime.																
4096	4096-bit Diffie-Hellman prime.																	
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																	
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																	
ssl-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable secure renegotiation.		
	<i>disable</i>	Disable secure renegotiation.		
url-map	URL pattern to match.	string	Maximum length: 511	/
url-map-type	Type of url-map.	option	-	sub-string
	Option	Description		
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.		
	<i>wildcard</i>	Match the pattern with wildcards.		
	<i>regex</i>	Match the pattern with a regular expression.		

config quic

Parameter	Description	Type	Size	Default						
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3						
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2						
active-migration	Enable/disable active migration (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable active migration.</td></tr><tr><td>disable</td><td>Disable active migration.</td></tr></table>				Option	Description	enable	Enable active migration.	disable	Disable active migration.
Option	Description									
enable	Enable active migration.									
disable	Disable active migration.									
grease-quic-bit	Enable/disable grease QUIC bit (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable grease QUIC bit.</td></tr><tr><td>disable</td><td>Disable grease QUIC bit.</td></tr></table>				Option	Description	enable	Enable grease QUIC bit.	disable	Disable grease QUIC bit.
Option	Description									
enable	Enable grease QUIC bit.									
disable	Disable grease QUIC bit.									

Parameter	Description	Type	Size	Default
max-ack-delay	Maximum ACK delay in milliseconds (1 - 16383, default = 25).	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes (1 - 1500, default = 1500).	integer	Minimum value: 1 Maximum value: 1500	1500
max-idle-timeout	Maximum idle timeout milliseconds (1 - 60000, default = 30000).	integer	Minimum value: 1 Maximum value: 60000	30000
max-udp-payload-size	Maximum UDP payload size in bytes (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500

config realservers

Parameter	Description	Type	Size	Default						
addr-type	Type of address.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Non-wildcard FQDN address object.</td></tr></table>	Option	Description	<i>ip</i>	Standard IPv4 address.	<i>fqdn</i>	Non-wildcard FQDN address object.			
Option	Description									
<i>ip</i>	Standard IPv4 address.									
<i>fqdn</i>	Non-wildcard FQDN address object.									
address	Address or address group of the real server.	string	Maximum length: 79							
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr></table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.			
Option	Description									
<i>disable</i>	Disable per server health check.									
<i>enable</i>	Enable per server health check.									
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>Use PING to test the link with the server.</td></tr><tr><td><i>http</i></td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td><i>tcp-connect</i></td><td>Use a full TCP connection to test the link with the server.</td></tr></table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.			
	Option	Description										
	<i>ping</i>	Use PING to test the link with the server.										
	<i>http</i>	Use HTTP-GET to test the link with the server.										
<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.											
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per server holddown.</td></tr><tr><td><i>disable</i></td><td>Disable per server holddown.</td></tr></table>	Option	Description	<i>enable</i>	Enable per server holddown.	<i>disable</i>	Disable per server holddown.					
	Option	Description										
	<i>enable</i>	Enable per server holddown.										
<i>disable</i>	Disable per server holddown.											
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295									
ip	IP address of the real server.	ipv4-address-any	Not Specified	0.0.0.0								
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Server status active.</td></tr><tr><td><i>standby</i></td><td>Server status standby.</td></tr><tr><td><i>disable</i></td><td>Server status disable.</td></tr></table>	Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.			
	Option	Description										
	<i>active</i>	Server status active.										
	<i>standby</i>	Server status standby.										
<i>disable</i>	Server status disable.											
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable virtual hostname/IP translation.</td></tr></table>	Option	Description	<i>enable</i>	Enable virtual hostname/IP translation.							
	Option	Description										
<i>enable</i>	Enable virtual hostname/IP translation.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable virtual hostname/IP translation.		
verify-cert	Enable/disable certificate verification of the real server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable certificate verification.		
	<i>disable</i>	Disable certificate verification.		
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	
	Option	Description		
	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.		
	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.		
	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	TLS-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
TLS-ECDHE-RSA-WITH-RC4-128-SHA	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.		
	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.		
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295	0
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3
	Option	Description		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config api-gateway6

Parameter	Description	Type	Size	Default
h2-support	HTTP2 support, default=Enable.	option	-	enable
	Option Description			
	enable Enable HTTP2 support.			
	disable Disable HTTP2 support.			
h3-support	HTTP3/QUIC support, default=Disable.	option	-	disable
	Option Description			
	enable Enable HTTP3/QUIC support.			
	disable Disable HTTP3/QUIC support.			
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	Option Description			
	disable Disable use of HTTP cookie domain from the host field in HTTP (use http-cooke-domain setting).			
	enable Enable use of HTTP cookie domain from the host field in HTTP.			
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35	
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	Option Description			
	disable Only allow HTTP cookie to match this API Gateway.			
	same-ip Allow HTTP cookie to match any API Gateway with the same IP.			

Parameter	Description	Type	Size	Default												
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark the cookie as secure. Allows sharing the cookie between HTTP and HTTPS connections.</td></tr><tr><td><i>enable</i></td><td>Mark the inserted cookie as secure. The cookie can only be used for HTTPS connections.</td></tr></table>	Option	Description	<i>disable</i>	Do not mark the cookie as secure. Allows sharing the cookie between HTTP and HTTPS connections.	<i>enable</i>	Mark the inserted cookie as secure. The cookie can only be used for HTTPS connections.									
Option	Description															
<i>disable</i>	Do not mark the cookie as secure. Allows sharing the cookie between HTTP and HTTPS connections.															
<i>enable</i>	Mark the inserted cookie as secure. The cookie can only be used for HTTPS connections.															
id	API Gateway ID.	integer	Minimum value: 0 0 Maximum value: 4294967295													
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute to servers based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute to servers based on round-robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute to servers based on weight.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to servers based on the host field in HTTP header.</td></tr></table>	Option	Description	<i>static</i>	Distribute to servers based on source IP.	<i>round-robin</i>	Distribute to servers based on round-robin order.	<i>weighted</i>	Distribute to servers based on weight.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to servers based on the host field in HTTP header.			
Option	Description															
<i>static</i>	Distribute to servers based on source IP.															
<i>round-robin</i>	Distribute to servers based on round-robin order.															
<i>weighted</i>	Distribute to servers based on weight.															
<i>first-alive</i>	Distribute to the first server that is alive.															
<i>http-host</i>	Distribute to servers based on the host field in HTTP header.															
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.									
Option	Description															
<i>none</i>	None.															
<i>http-cookie</i>	HTTP cookie.															
service	Service.	option	-	https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.									
Option	Description															
<i>http</i>	HTTP.															
<i>https</i>	HTTPS.															
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high												

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.									
	Option	Description																
	<i>high</i>	High encryption. Allow only AES and ChaCha.																
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td><i>3072</i></td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td><i>4096</i></td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.			
	Option	Description																
	<i>768</i>	768-bit Diffie-Hellman prime.																
	<i>1024</i>	1024-bit Diffie-Hellman prime.																
	<i>1536</i>	1536-bit Diffie-Hellman prime.																
	<i>2048</i>	2048-bit Diffie-Hellman prime.																
	<i>3072</i>	3072-bit Diffie-Hellman prime.																
<i>4096</i>	4096-bit Diffie-Hellman prime.																	
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																	
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																	
ssl-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable secure renegotiation.		
	<i>disable</i>	Disable secure renegotiation.		
url-map	URL pattern to match.	string	Maximum length: 511	/
url-map-type	Type of url-map.	option	-	sub-string
	Option	Description		
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.		
	<i>wildcard</i>	Match the pattern with wildcards.		
	<i>regex</i>	Match the pattern with a regular expression.		

config quic

Parameter	Description	Type	Size	Default						
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3						
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2						
active-migration	Enable/disable active migration (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable active migration.</td></tr><tr><td>disable</td><td>Disable active migration.</td></tr></table>				Option	Description	enable	Enable active migration.	disable	Disable active migration.
Option	Description									
enable	Enable active migration.									
disable	Disable active migration.									
grease-quic-bit	Enable/disable grease QUIC bit (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable grease QUIC bit.</td></tr><tr><td>disable</td><td>Disable grease QUIC bit.</td></tr></table>				Option	Description	enable	Enable grease QUIC bit.	disable	Disable grease QUIC bit.
Option	Description									
enable	Enable grease QUIC bit.									
disable	Disable grease QUIC bit.									

Parameter	Description	Type	Size	Default
max-ack-delay	Maximum ACK delay in milliseconds (1 - 16383, default = 25).	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes (1 - 1500, default = 1500).	integer	Minimum value: 1 Maximum value: 1500	1500
max-idle-timeout	Maximum idle timeout milliseconds (1 - 60000, default = 30000).	integer	Minimum value: 1 Maximum value: 60000	30000
max-udp-payload-size	Maximum UDP payload size in bytes (1200 - 1500, default = 1500).	integer	Minimum value: 1200 Maximum value: 1500	1500

config realservers

Parameter	Description	Type	Size	Default						
addr-type	Type of address.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Non-wildcard FQDN address object.</td></tr></table>	Option	Description	<i>ip</i>	Standard IPv4 address.	<i>fqdn</i>	Non-wildcard FQDN address object.			
Option	Description									
<i>ip</i>	Standard IPv4 address.									
<i>fqdn</i>	Non-wildcard FQDN address object.									
address	Address or address group of the real server.	string	Maximum length: 79							
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr></table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.			
Option	Description									
<i>disable</i>	Disable per server health check.									
<i>enable</i>	Enable per server health check.									
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping						

Parameter	Description	Type	Size	Default									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>Use PING to test the link with the server.</td></tr><tr><td><i>http</i></td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td><i>tcp-connect</i></td><td>Use a full TCP connection to test the link with the server.</td></tr></table>		Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.			
	Option	Description											
	<i>ping</i>	Use PING to test the link with the server.											
	<i>http</i>	Use HTTP-GET to test the link with the server.											
<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.												
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per server holddown.</td></tr><tr><td><i>disable</i></td><td>Disable per server holddown.</td></tr></table>		Option	Description	<i>enable</i>	Enable per server holddown.	<i>disable</i>	Disable per server holddown.					
	Option	Description											
	<i>enable</i>	Enable per server holddown.											
<i>disable</i>	Disable per server holddown.												
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63										
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0									
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::									
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443									
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Server status active.</td></tr><tr><td><i>standby</i></td><td>Server status standby.</td></tr><tr><td><i>disable</i></td><td>Server status disable.</td></tr></table>		Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.			
	Option	Description											
	<i>active</i>	Server status active.											
	<i>standby</i>	Server status standby.											
<i>disable</i>	Server status disable.												
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable virtual hostname/IP translation.</td></tr><tr><td><i>disable</i></td><td>Disable virtual hostname/IP translation.</td></tr></table>		Option	Description	<i>enable</i>	Enable virtual hostname/IP translation.	<i>disable</i>	Disable virtual hostname/IP translation.					
	Option	Description											
	<i>enable</i>	Enable virtual hostname/IP translation.											
<i>disable</i>	Disable virtual hostname/IP translation.												

Parameter	Description	Type	Size	Default
verify-cert	Enable/disable certificate verification of the real server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable certificate verification.		
	<i>disable</i>	Disable certificate verification.		
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	
	Option	Description		
	<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.		
	<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.		
	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		
	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.</td></tr></table>	Option	Description	TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.	TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.			
Option	Description																											
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																											
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																											
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																											
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																											
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																											
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																											
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																											
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																											
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																											
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.																											
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		
TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		
	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.		
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																		
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																			
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 0 Maximum value: 4294967295																	
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.									
	Option	Description																		
	<i>tls-1.0</i>	TLS 1.0.																		
	<i>tls-1.1</i>	TLS 1.1.																		
	<i>tls-1.2</i>	TLS 1.2.																		
<i>tls-1.3</i>	TLS 1.3.																			

CLI diagnose commands

Use diagnose commands to run debugging commands.

This section includes syntax for the following commands:

- [diagnose alertconsole on page 2711](#)
- [diagnose antivirus on page 2712](#)
- [diagnose automation on page 2714](#)
- [diagnose autoupdate on page 2714](#)
- [diagnose azure events on page 2715](#)
- [diagnose casb on page 2716](#)
- [diagnose central-mgmt on page 2719](#)
- [diagnose cid on page 2720](#)
- [diagnose clearpass on page 2724](#)
- [diagnose debug on page 2726](#)
- [diagnose disktest on page 2802](#)
- [diagnose dpdk config on page 2804](#)
- [diagnose dpdk log clear on page 2804](#)
- [diagnose dpdk log show on page 2805](#)
- [diagnose dpdk performance on page 2805](#)
- [diagnose dpdk statistics clear on page 2805](#)
- [diagnose dpdk statistics show on page 2806](#)
- [diagnose dpdk version on page 2807](#)
- [diagnose emailfilter on page 2807](#)
- [diagnose endpoint on page 2809](#)
- [diagnose extender on page 2829](#)
- [diagnose fdsm on page 2830](#)
- [diagnose ffdb-fqdn on page 2837](#)
- [diagnose firewall on page 2838](#)
- [diagnose forticare on page 2895](#)
- [diagnose fortiguard-resources on page 2897](#)
- [diagnose fortimq on page 2911](#)
- [diagnose fortism on page 2912](#)
- [diagnose fortitoken-cloud on page 2914](#)
- [diagnose fortitoken on page 2912](#)
- [diagnose fortiview on page 2917](#)
- [diagnose geoip on page 2918](#)
- [diagnose hardware on page 2919](#)
- [diagnose internet-service-name on page 2927](#)
- [diagnose internet-service on page 2924](#)

- [diagnose internet-service6 on page 2926](#)
- [diagnose ip address on page 2928](#)
- [diagnose ip arp on page 2929](#)
- [diagnose ip gre-tunnel on page 2930](#)
- [diagnose ip ipip-tunnel on page 2930](#)
- [diagnose ip multicast on page 2931](#)
- [diagnose ip parp on page 2933](#)
- [diagnose ip proute on page 2933](#)
- [diagnose ip route on page 2934](#)
- [diagnose ip router bfd on page 2936](#)
- [diagnose ip router bgp on page 2938](#)
- [diagnose ip router command on page 2941](#)
- [diagnose ip router igmp on page 2942](#)
- [diagnose ip router isis on page 2944](#)
- [diagnose ip router ospf on page 2947](#)
- [diagnose ip router pim-dm on page 2950](#)
- [diagnose ip router pim-sm on page 2953](#)
- [diagnose ip router rip on page 2961](#)
- [diagnose ip router zl on page 2964](#)
- [diagnose ip rtcache on page 2964](#)
- [diagnose ip tcp on page 2965](#)
- [diagnose ip udp on page 2965](#)
- [diagnose ips anomaly on page 2965](#)
- [diagnose ips anomaly6 on page 2968](#)
- [diagnose ips av avengine on page 2970](#)
- [diagnose ips av cache on page 2971](#)
- [diagnose ips av mode on page 2972](#)
- [diagnose ips av query on page 2973](#)
- [diagnose ips av stats on page 2973](#)
- [diagnose ips av timeout on page 2974](#)
- [diagnose ips config disable on page 2974](#)
- [diagnose ips config enable on page 2975](#)
- [diagnose ips dac on page 2975](#)
- [diagnose ips debug disable on page 2976](#)
- [diagnose ips debug enable on page 2983](#)
- [diagnose ips debug level on page 2990](#)
- [diagnose ips debug status on page 2990](#)
- [diagnose ips debug timelimit on page 2991](#)
- [diagnose ips dissector on page 2991](#)
- [diagnose ips filter on page 2992](#)
- [diagnose ips global rule on page 2993](#)
- [diagnose ips gtp on page 2994](#)
- [diagnose ips ipsa on page 2995](#)

- [diagnose ips l2ips on page 2995](#)
- [diagnose ips memory on page 2996](#)
- [diagnose ips packet on page 2997](#)
- [diagnose ips pme debug on page 2998](#)
- [diagnose ips pme detail on page 2999](#)
- [diagnose ips pme dynamic-address on page 3001](#)
- [diagnose ips pme fabric-address on page 3001](#)
- [diagnose ips pme policy on page 3002](#)
- [diagnose ips raw on page 3003](#)
- [diagnose ips session on page 3003](#)
- [diagnose ips share on page 3004](#)
- [diagnose ips shmopts on page 3005](#)
- [diagnose ips signature on page 3006](#)
- [diagnose ips ssl on page 3007](#)
- [diagnose ips tcp on page 3010](#)
- [diagnose ips test on page 3010](#)
- [diagnose ips urlfilter on page 3011](#)
- [diagnose ips vpatch on page 3011](#)
- [diagnose ipv6 address on page 3012](#)
- [diagnose ipv6 devconf on page 3014](#)
- [diagnose ipv6 gre-tunnel on page 3014](#)
- [diagnose ipv6 ipv6-tunnel on page 3015](#)
- [diagnose ipv6 multicast on page 3015](#)
- [diagnose ipv6 neighbor-cache on page 3016](#)
- [diagnose ipv6 proute on page 3017](#)
- [diagnose ipv6 route on page 3018](#)
- [diagnose ipv6 router ospf on page 3018](#)
- [diagnose ipv6 router pim-sm on page 3021](#)
- [diagnose ipv6 router rip on page 3029](#)
- [diagnose ipv6 router zl6 on page 3031](#)
- [diagnose ipv6 sit-tunnel on page 3032](#)
- [diagnose l2vpn evpn on page 3032](#)
- [diagnose lldp on page 3035](#)
- [diagnose log on page 3039](#)
- [diagnose netlink aggregate on page 3043](#)
- [diagnose netlink backlog on page 3044](#)
- [diagnose netlink brctl on page 3045](#)
- [diagnose netlink device on page 3046](#)
- [diagnose netlink dstmac on page 3046](#)
- [diagnose netlink interface on page 3047](#)
- [diagnose netlink intf-class on page 3049](#)
- [diagnose netlink intf-qdisc on page 3049](#)
- [diagnose netlink qlen on page 3049](#)

- [diagnose netlink redundant on page 3050](#)
- [diagnose nodejs on page 3051](#)
- [diagnose oci on page 3053](#)
- [diagnose on-demand-sniffer on page 3054](#)
- [diagnose radiusd on page 3055](#)
- [diagnose report-runner-v2 on page 3058](#)
- [diagnose report-runner on page 3057](#)
- [diagnose report on page 3055](#)
- [diagnose rsso on page 3059](#)
- [diagnose saas on page 3062](#)
- [diagnose settings on page 3063](#)
- [diagnose sladb on page 3064](#)
- [diagnose sniffer on page 3065](#)
- [diagnose snmp ip on page 3069](#)
- [diagnose snmp ip6 on page 3070](#)
- [diagnose snmp net on page 3071](#)
- [diagnose snmp trap on page 3072](#)
- [diagnose switch-controller on page 3072](#)
- [diagnose sys on page 3110](#)
- [diagnose test analytics-pdf-report on page 3336](#)
- [diagnose test analytics-report on page 3337](#)
- [diagnose test application on page 3337](#)
- [diagnose test authserver on page 3359](#)
- [diagnose test guest on page 3362](#)
- [diagnose test scim on page 3362](#)
- [diagnose test security on page 3364](#)
- [diagnose test update on page 3364](#)
- [diagnose traffictest on page 3365](#)
- [diagnose user-device-store on page 3372](#)
- [diagnose user on page 3367](#)
- [diagnose vendor-mac on page 3388](#)
- [diagnose vpn ike on page 3389](#)
- [diagnose vpn ikecrypt on page 3410](#)
- [diagnose vpn ipsec on page 3412](#)
- [diagnose vpn l2tp on page 3413](#)
- [diagnose vpn mr on page 3413](#)
- [diagnose vpn mr6 on page 3415](#)
- [diagnose vpn pptp on page 3417](#)
- [diagnose vpn ssl on page 3417](#)
- [diagnose vpn tunnel on page 3426](#)
- [diagnose wacs on page 3431](#)
- [diagnose wad on page 3431](#)
- [diagnose wadbd on page 3572](#)

- [diagnose waf on page 3572](#)
- [diagnose web-ui on page 3577](#)
- [diagnose webfilter bword on page 3573](#)
- [diagnose webfilter fortiguard on page 3573](#)
- [diagnose webfilter quota on page 3576](#)
- [diagnose webfilter stats on page 3577](#)
- [diagnose wireless-controller on page 3582](#)
- [diagnose wpa on page 3583](#)

diagnose alertconsole

alertconsole

This topic includes the following commands:

- [diagnose alertconsole clear on page 2711](#)
- [diagnose alertconsole fgd-retrieve on page 2711](#)
- [diagnose alertconsole list on page 2711](#)
- [diagnose alertconsole test on page 2712](#)

diagnose alertconsole clear

Clear alert messages.

```
diagnose alertconsole clear
```

diagnose alertconsole fgd-retrieve

Retrieve FortiGuard alerts.

```
diagnose alertconsole fgd-retrieve
```

diagnose alertconsole list

List current alert messages.

```
diagnose alertconsole list
```

diagnose alertconsole test

Generate alert messages.

```
diagnose alertconsole test
```

diagnose antivirus

antivirus

This topic includes the following commands:

- [diagnose antivirus database-info on page 2712](#)
- [diagnose antivirus outbreak-prevention on page 2712](#)
- [diagnose antivirus outbreak-prevention statistics on page 2712](#)
- [diagnose antivirus outbreak-prevention statistics flush on page 2713](#)
- [diagnose antivirus outbreak-prevention statistics list on page 2713](#)
- [diagnose antivirus quarantine on page 2713](#)
- [diagnose antivirus quarantine delete on page 2713](#)
- [diagnose antivirus quarantine list on page 2713](#)
- [diagnose antivirus quarantine purge on page 2714](#)
- [diagnose antivirus test on page 2714](#)

diagnose antivirus database-info

AntiVirus database info.

```
diagnose antivirus database-info
```

diagnose antivirus outbreak-prevention

FortiGuard - Virus Outbreak Prevention statistics and reporting.

```
diagnose antivirus outbreak-prevention
```

diagnose antivirus outbreak-prevention statistics

Cache and daemon statistics.

```
diagnose antivirus outbreak-prevention statistics
```


diagnose antivirus outbreak-prevention statistics flush

Flush daemon and cache statistics.

```
diagnose antivirus outbreak-prevention statistics flush
```

diagnose antivirus outbreak-prevention statistics list

Display cache and daemon statistics.

```
diagnose antivirus outbreak-prevention statistics list
```

diagnose antivirus quarantine

Quarantine functions.

```
diagnose antivirus quarantine
```

diagnose antivirus quarantine delete

Delete a file in quarantine.

```
diagnose antivirus quarantine delete <checksum>
```

Parameter	Description	Type	Size
<checksum>	Checksum of the file to delete.	string	

diagnose antivirus quarantine list

List the files in quarantine.

```
diagnose antivirus quarantine list <value>
```

Parameter	Description	Type	Size
<value>	service: http, https, ftp, smtp, smtps, pop3, pop3s, imap, imaps, im, nntp status: infected, machine-learning, blocked (optional)	string	

diagnose antivirus quarantine purge

Delete all quarantined files.

```
diagnose antivirus quarantine purge
```

diagnose antivirus test

AV Engine diagnostics.

```
diagnose antivirus test <command>
```

Parameter	Description	Type	Size
<command>	Command to pass into AV engine. Please double quote the command.	string	

diagnose automation

Diagnose commands for automation stitches.

This topic includes the following commands:

- [diagnose automation test on page 2714](#)

diagnose automation test

Test automation stitches.

```
diagnose automation test
```

diagnose autoupdate

Automatic updates.

This topic includes the following commands:

- [diagnose autoupdate downgrade on page 2715](#)
- [diagnose autoupdate downgrade disable on page 2715](#)
- [diagnose autoupdate downgrade enable on page 2715](#)

- [diagnose autoupdate status on page 2715](#)
- [diagnose autoupdate versions on page 2715](#)

diagnose autoupdate downgrade

Update object downgrade status.

```
diagnose autoupdate downgrade
```

diagnose autoupdate downgrade disable

Disable Update object downgrade.

```
diagnose autoupdate downgrade disable
```

diagnose autoupdate downgrade enable

Enable Update object downgrade.

```
diagnose autoupdate downgrade enable
```

diagnose autoupdate status

Status of automatic updates.

```
diagnose autoupdate status
```

diagnose autoupdate versions

Update object versions.

```
diagnose autoupdate versions
```

diagnose azure events

Show azure scheduled events

This topic includes the following commands:

- [diagnose azure events migration on page 2716](#)

diagnose azure events migration

Show migration events.

```
diagnose azure events migration
```

diagnose casb

CASB diagnose commands.

This topic includes the following commands:

- [diagnose casb build on page 2716](#)
- [diagnose casb show on page 2716](#)
- [diagnose casb show app-attributes on page 2717](#)
- [diagnose casb show app-details on page 2717](#)
- [diagnose casb show app-domains on page 2717](#)
- [diagnose casb show applications on page 2717](#)
- [diagnose casb show apps on page 2717](#)
- [diagnose casb show domains on page 2717](#)
- [diagnose casb show isdb on page 2718](#)
- [diagnose casb show isdb-all on page 2718](#)
- [diagnose casb show isdb-name on page 2718](#)
- [diagnose casb show isdb-uuid on page 2718](#)
- [diagnose casb verify on page 2718](#)
- [diagnose casb verify casb-isdb on page 2718](#)

diagnose casb build

Test to build the CASB database.

```
diagnose casb build
```

diagnose casb show

Show CASB database.

```
diagnose casb show
```

diagnose casb show app-attributes

Show built-in CASB application attributes by name.

```
diagnose casb show app-attributes
```

diagnose casb show app-details

Show built-in CASB application details by name.

```
diagnose casb show app-details
```

diagnose casb show app-domains

Show built-in CASB application domains by name.

```
diagnose casb show app-domains
```

diagnose casb show applications

Show all built-in CASB application details.

```
diagnose casb show applications
```

diagnose casb show apps

Show built-in CASB application list.

```
diagnose casb show apps
```

diagnose casb show domains

Show all built-in CASB domains.

```
diagnose casb show domains
```

diagnose casb show isdb

Show built-in CASB-ISDB mapping database.

```
diagnose casb show isdb
```

diagnose casb show isdb-all

Show all built-in CASB-ISDB mappings.

```
diagnose casb show isdb-all
```

diagnose casb show isdb-name

Show built-in CASB-ISDB mapping by application name.

```
diagnose casb show isdb-name
```

diagnose casb show isdb-uuid

Show built-in CASB-ISDB mapping by application UUID.

```
diagnose casb show isdb-uuid
```

diagnose casb verify

Verify databases.

```
diagnose casb verify
```

diagnose casb verify casb-isdb

Verify the CASB database with CASB-ISDB mapping database.

```
diagnose casb verify casb-isdb
```

diagnose central-mgmt

Central management.

This topic includes the following commands:

- [diagnose central-mgmt script-history on page 2719](#)
- [diagnose central-mgmt script-history clear on page 2719](#)
- [diagnose central-mgmt script-history del on page 2719](#)
- [diagnose central-mgmt script-history list on page 2719](#)
- [diagnose central-mgmt script-history test on page 2720](#)

diagnose central-mgmt script-history

Script execution history.

```
diagnose central-mgmt script-history
```

diagnose central-mgmt script-history clear

Clear script execution history.

```
diagnose central-mgmt script-history clear
```

diagnose central-mgmt script-history del

Delete one script execution record.

```
diagnose central-mgmt script-history del <id>
```

Parameter	Description	Type	Size
<id>	Record ID.	string	

diagnose central-mgmt script-history list

List script execution history.

```
diagnose central-mgmt script-history list
```

diagnose central-mgmt script-history test

Generate sample script execution records.

```
diagnose central-mgmt script-history test
```

diagnose cid

Device Identification diagnostics.

This topic includes the following commands:

- [diagnose cid debug on page 2720](#)
- [diagnose cid debug filter on page 2721](#)
- [diagnose cid debug filter clear on page 2721](#)
- [diagnose cid debug filter clear mac on page 2721](#)
- [diagnose cid debug filter mac on page 2721](#)
- [diagnose cid debug start on page 2721](#)
- [diagnose cid debug stop on page 2721](#)
- [diagnose cid restart on page 2722](#)
- [diagnose cid scan on page 2722](#)
- [diagnose cid scan csf on page 2722](#)
- [diagnose cid scan ethernet on page 2722](#)
- [diagnose cid scan lldp on page 2723](#)
- [diagnose cid stats on page 2723](#)
- [diagnose cid stats config on page 2723](#)
- [diagnose cid stats crash on page 2723](#)
- [diagnose cid stats debug on page 2723](#)
- [diagnose cid stats manager on page 2724](#)
- [diagnose cid stats scan on page 2724](#)
- [diagnose cid stats trap on page 2724](#)
- [diagnose cid stats unpack on page 2724](#)

diagnose cid debug

Control debug log for cid.

```
diagnose cid debug
```


diagnose cid debug filter

Show the filter for this console.

```
diagnose cid debug filter
```

diagnose cid debug filter clear

Clear the filter.

```
diagnose cid debug filter clear
```

diagnose cid debug filter clear mac

Clear the MAC filter.

```
diagnose cid debug filter clear mac
```

diagnose cid debug filter mac

Source or destination MAC address to match.

```
diagnose cid debug filter mac
```

diagnose cid debug start

Start logging cid debug on this console.

```
diagnose cid debug start
```

diagnose cid debug stop

Stop logging cid debug on this console.

```
diagnose cid debug stop
```

diagnose cid restart

Restart cid.

```
diagnose cid restart
```

diagnose cid scan

Scan something

```
diagnose cid scan
```

diagnose cid scan csf

Scan Fortinet serial number (SN) as if it came from CSF

```
diagnose cid scan csf <interface> <ip4-address> <serial-number>
```

Parameter	Description	Type	Size
<interface>	Interface the device is connected to.	string	
<ip4-address>	IPv4 address of the device	string	
<serial-number>	Fortinet device serial number (SN)	string	

diagnose cid scan ethernet

Scan a hex-encoded ethernet packet

```
diagnose cid scan ethernet <hex-encoded-ethernet-packet>
```

Parameter	Description	Type	Size
<hex-encoded-ethernet-packet>	Hex encoded Ethernet packet.	string	

diagnose cid scan lldp

Scan LLDP

```
diagnose cid scan lldp <mac> <ipv4-address> <system-name> <system-description> <model>
```

Parameter	Description	Type	Size
<mac>	MAC address	string	
<ipv4-address>	LLDP IPv4 Management address	string	
<system-name>	LLDP System Name	string	
<system-description>	LLDP System Description	string	
<model>	LLDP Model	string	

diagnose cid stats

Device Identification statistics.

```
diagnose cid stats
```

diagnose cid stats config

Device Identification statistics for the configuration handling.

```
diagnose cid stats config
```

diagnose cid stats crash

Device Identification statistics for the crash log.

```
diagnose cid stats crash
```

diagnose cid stats debug

Device Identification statistics for the debug log.

```
diagnose cid stats debug
```

diagnose cid stats manager

Device Identification statistics for the manager.

```
diagnose cid stats manager
```

diagnose cid stats scan

Device Identification statistics for the traffic scanner.

```
diagnose cid stats scan
```

diagnose cid stats trap

Device Identification statistics for the SNMP trap generator.

```
diagnose cid stats trap
```

diagnose cid stats unpack

Device Identification statistics for the signature unpacker.

```
diagnose cid stats unpack
```

diagnose clearpass

ClearPass service SPT (System Posture Token) information.

This topic includes the following commands:

- [diagnose clearpass delete on page 2725](#)
- [diagnose clearpass flush on page 2725](#)
- [diagnose clearpass list on page 2725](#)
- [diagnose clearpass list address on page 2725](#)
- [diagnose clearpass list spt on page 2725](#)
- [diagnose clearpass list summary on page 2726](#)

diagnose clearpass delete

Delete ClearPass database by IP address.

```
diagnose clearpass delete <IP>
```

Parameter	Description	Type	Size
<IP>	IP address	string	

diagnose clearpass flush

Delete ClearPass database.

```
diagnose clearpass flush
```

diagnose clearpass list

List ClearPass database.

```
diagnose clearpass list
```

diagnose clearpass list address

List by IP address.

```
diagnose clearpass list address <IP>
```

Parameter	Description	Type	Size
<IP>	IP address	string	

diagnose clearpass list spt

List by SPT value.

```
diagnose clearpass list spt <spt-value>
```

Parameter	Description	Type	Size
<spt-value>	SPT value	string	

diagnose clearpass list summary

List summary of the ClearPass database.

```
diagnose clearpass list summary
```

diagnose debug

debug

This topic includes the following commands:

- [diagnose debug admin on page 2733](#)
- [diagnose debug admin error-log on page 2734](#)
- [diagnose debug application on page 2734](#)
- [diagnose debug application acd on page 2734](#)
- [diagnose debug application acid on page 2734](#)
- [diagnose debug application alarmd on page 2734](#)
- [diagnose debug application alertmail on page 2735](#)
- [diagnose debug application alicloud-ha on page 2735](#)
- [diagnose debug application alicloud-sdn on page 2735](#)
- [diagnose debug application authd on page 2735](#)
- [diagnose debug application autod on page 2736](#)
- [diagnose debug application awsd on page 2736](#)
- [diagnose debug application azd on page 2736](#)
- [diagnose debug application azd-ha on page 2736](#)
- [diagnose debug application bfdd on page 2737](#)
- [diagnose debug application cert-update on page 2737](#)
- [diagnose debug application chassis on page 2737](#)
- [diagnose debug application clearpass on page 2737](#)
- [diagnose debug application cloudapid on page 2738](#)
- [diagnose debug application cloudinitd on page 2738](#)
- [diagnose debug application cmp on page 2738](#)
- [diagnose debug application crl-update on page 2738](#)
- [diagnose debug application csfd on page 2738](#)
- [diagnose debug application cu_acd on page 2739](#)
- [diagnose debug application cw_acd on page 2739](#)
- [diagnose debug application cw_acd_helper on page 2739](#)
- [diagnose debug application cw_acd_wlev on page 2740](#)
- [diagnose debug application cw_acd_wpad on page 2740](#)
- [diagnose debug application ddnsd on page 2740](#)
- [diagnose debug application dhcp6c on page 2740](#)

- [diagnose debug application dhcp6r on page 2741](#)
- [diagnose debug application dhcp6s on page 2741](#)
- [diagnose debug application dhcpc on page 2741](#)
- [diagnose debug application dhcprelay on page 2741](#)
- [diagnose debug application dhcps on page 2741](#)
- [diagnose debug application dlpfingerprint on page 2742](#)
- [diagnose debug application dnp on page 2742](#)
- [diagnose debug application dnsproxy on page 2742](#)
- [diagnose debug application eap_proxy on page 2742](#)
- [diagnose debug application eap_supp on page 2743](#)
- [diagnose debug application est on page 2743](#)
- [diagnose debug application evpnd on page 2743](#)
- [diagnose debug application extenderd on page 2743](#)
- [diagnose debug application fclfd on page 2744](#)
- [diagnose debug application fcnacd on page 2744](#)
- [diagnose debug application fds_notify on page 2744](#)
- [diagnose debug application fgd_alert on page 2744](#)
- [diagnose debug application fgfmd on page 2744](#)
- [diagnose debug application fgtlogd on page 2745](#)
- [diagnose debug application flcfgd on page 2745](#)
- [diagnose debug application flpold on page 2745](#)
- [diagnose debug application fltund on page 2745](#)
- [diagnose debug application fnbamd on page 2746](#)
- [diagnose debug application foauthd on page 2746](#)
- [diagnose debug application forticldd on page 2746](#)
- [diagnose debug application forticron on page 2746](#)
- [diagnose debug application fortilinkd on page 2747](#)
- [diagnose debug application fortimq on page 2747](#)
- [diagnose debug application fsso_ldap on page 2747](#)
- [diagnose debug application fssod on page 2747](#)
- [diagnose debug application fsvrd on page 2747](#)
- [diagnose debug application ftm-push on page 2748](#)
- [diagnose debug application garpd on page 2748](#)
- [diagnose debug application gcpcd on page 2748](#)
- [diagnose debug application hamonitord on page 2748](#)
- [diagnose debug application harelay on page 2749](#)
- [diagnose debug application hasync on page 2749](#)
- [diagnose debug application hataik on page 2749](#)
- [diagnose debug application httpsd on page 2749](#)
- [diagnose debug application ibmd on page 2750](#)
- [diagnose debug application icond on page 2750](#)
- [diagnose debug application ike on page 2750](#)
- [diagnose debug application ikecrypt on page 2750](#)

- [diagnose debug application imap on page 2751](#)
- [diagnose debug application init on page 2751](#)
- [diagnose debug application iotd on page 2751](#)
- [diagnose debug application ipamd on page 2751](#)
- [diagnose debug application ipamsd on page 2752](#)
- [diagnose debug application ipldbd on page 2752](#)
- [diagnose debug application ipsengine on page 2752](#)
- [diagnose debug application ipsmonitor on page 2752](#)
- [diagnose debug application ipsufd on page 2752](#)
- [diagnose debug application kmiglogd on page 2753](#)
- [diagnose debug application kmipd on page 2753](#)
- [diagnose debug application kubed on page 2753](#)
- [diagnose debug application l2tp on page 2753](#)
- [diagnose debug application link-monitor on page 2754](#)
- [diagnose debug application link-monitor-passive on page 2754](#)
- [diagnose debug application locallogd on page 2754](#)
- [diagnose debug application lpmd on page 2754](#)
- [diagnose debug application miglogd on page 2755](#)
- [diagnose debug application mrd on page 2755](#)
- [diagnose debug application netxd on page 2755](#)
- [diagnose debug application nntp on page 2755](#)
- [diagnose debug application nodejs on page 2755](#)
- [diagnose debug application npd on page 2756](#)
- [diagnose debug application ntnxd on page 2756](#)
- [diagnose debug application ntpd on page 2756](#)
- [diagnose debug application oaas_agent on page 2756](#)
- [diagnose debug application ocid on page 2757](#)
- [diagnose debug application openstackd on page 2757](#)
- [diagnose debug application ovrd on page 2757](#)
- [diagnose debug application pcpd on page 2757](#)
- [diagnose debug application pop3 on page 2758](#)
- [diagnose debug application ppp on page 2758](#)
- [diagnose debug application pppoed on page 2758](#)
- [diagnose debug application pptp on page 2758](#)
- [diagnose debug application pptpc on page 2758](#)
- [diagnose debug application proxy on page 2759](#)
- [diagnose debug application ptpd on page 2759](#)
- [diagnose debug application quarantine on page 2759](#)
- [diagnose debug application radius-das on page 2759](#)
- [diagnose debug application radiusd on page 2760](#)
- [diagnose debug application radvd on page 2760](#)
- [diagnose debug application reportd on page 2760](#)
- [diagnose debug application route-tag on page 2760](#)

- [diagnose debug application samld on page 2761](#)
- [diagnose debug application sapd on page 2761](#)
- [diagnose debug application sccp on page 2761](#)
- [diagnose debug application scep on page 2761](#)
- [diagnose debug application scimd on page 2762](#)
- [diagnose debug application sdncd on page 2762](#)
- [diagnose debug application sdnvpnd on page 2762](#)
- [diagnose debug application sdwan on page 2762](#)
- [diagnose debug application sepmd on page 2762](#)
- [diagnose debug application server-probe on page 2763](#)
- [diagnose debug application sessionsync on page 2763](#)
- [diagnose debug application sflowd on page 2763](#)
- [diagnose debug application sfupgraded on page 2763](#)
- [diagnose debug application sip on page 2764](#)
- [diagnose debug application smbcd on page 2764](#)
- [diagnose debug application smtp on page 2764](#)
- [diagnose debug application snmpd on page 2764](#)
- [diagnose debug application spareblock on page 2765](#)
- [diagnose debug application speedtest on page 2765](#)
- [diagnose debug application speedtestd on page 2765](#)
- [diagnose debug application sshd on page 2765](#)
- [diagnose debug application sslvpn on page 2765](#)
- [diagnose debug application syslogd on page 2766](#)
- [diagnose debug application update on page 2766](#)
- [diagnose debug application uploadd on page 2766](#)
- [diagnose debug application urlfilter on page 2766](#)
- [diagnose debug application vmwd on page 2767](#)
- [diagnose debug application vned on page 2767](#)
- [diagnose debug application vrrpd on page 2767](#)
- [diagnose debug application wabcs on page 2767](#)
- [diagnose debug application waocs on page 2768](#)
- [diagnose debug application wccpd on page 2768](#)
- [diagnose debug application wf_monitor on page 2768](#)
- [diagnose debug application wifi on page 2768](#)
- [diagnose debug application wpa-show-keys on page 2768](#)
- [diagnose debug application wpa-timestamp on page 2769](#)
- [diagnose debug application wpad on page 2769](#)
- [diagnose debug application wpad-crash-hexdump on page 2769](#)
- [diagnose debug application zebos on page 2769](#)
- [diagnose debug application zebos-launcher on page 2770](#)
- [diagnose debug authd on page 2770](#)
- [diagnose debug authd clear on page 2770](#)
- [diagnose debug authd fsso on page 2770](#)

- [diagnose debug authd fsso add-address on page 2770](#)
- [diagnose debug authd fsso clear-logons on page 2771](#)
- [diagnose debug authd fsso del-address on page 2771](#)
- [diagnose debug authd fsso filter on page 2771](#)
- [diagnose debug authd fsso filter clear on page 2771](#)
- [diagnose debug authd fsso filter group on page 2772](#)
- [diagnose debug authd fsso filter server on page 2772](#)
- [diagnose debug authd fsso filter source on page 2772](#)
- [diagnose debug authd fsso filter user on page 2772](#)
- [diagnose debug authd fsso flush-address on page 2773](#)
- [diagnose debug authd fsso flush-address-all on page 2773](#)
- [diagnose debug authd fsso list on page 2773](#)
- [diagnose debug authd fsso refresh-groups on page 2773](#)
- [diagnose debug authd fsso refresh-logons on page 2773](#)
- [diagnose debug authd fsso server-status on page 2773](#)
- [diagnose debug authd fsso show-address on page 2774](#)
- [diagnose debug authd fsso summary on page 2774](#)
- [diagnose debug authd memory on page 2774](#)
- [diagnose debug aws-vpce on page 2774](#)
- [diagnose debug backtrace on page 2774](#)
- [diagnose debug cli on page 2774](#)
- [diagnose debug cloudinit on page 2775](#)
- [diagnose debug cloudinit clear on page 2775](#)
- [diagnose debug cloudinit show on page 2775](#)
- [diagnose debug cmdb-trace on page 2775](#)
- [diagnose debug cmdb-walk on page 2775](#)
- [diagnose debug config-error-log on page 2776](#)
- [diagnose debug config-error-log clear on page 2776](#)
- [diagnose debug config-error-log read on page 2776](#)
- [diagnose debug console on page 2776](#)
- [diagnose debug console no-user-log-msg on page 2776](#)
- [diagnose debug console no-user-log-msg disable on page 2776](#)
- [diagnose debug console no-user-log-msg enable on page 2777](#)
- [diagnose debug console retry-log-msg on page 2777](#)
- [diagnose debug console retry-log-msg disable on page 2777](#)
- [diagnose debug console retry-log-msg enable on page 2777](#)
- [diagnose debug console send on page 2777](#)
- [diagnose debug console timestamp on page 2778](#)
- [diagnose debug console timestamp disable on page 2778](#)
- [diagnose debug console timestamp enable on page 2778](#)
- [diagnose debug crashlog on page 2778](#)
- [diagnose debug crashlog clear on page 2778](#)
- [diagnose debug crashlog get on page 2778](#)

- [diagnose debug crashlog history on page 2779](#)
- [diagnose debug crashlog interval on page 2779](#)
- [diagnose debug disable on page 2779](#)
- [diagnose debug duration on page 2779](#)
- [diagnose debug enable on page 2779](#)
- [diagnose debug flow on page 2780](#)
- [diagnose debug flow filter on page 2780](#)
- [diagnose debug flow filter addr on page 2780](#)
- [diagnose debug flow filter clear on page 2780](#)
- [diagnose debug flow filter daddr on page 2780](#)
- [diagnose debug flow filter dport on page 2781](#)
- [diagnose debug flow filter negate on page 2781](#)
- [diagnose debug flow filter negate addr on page 2781](#)
- [diagnose debug flow filter negate daddr on page 2781](#)
- [diagnose debug flow filter negate dport on page 2781](#)
- [diagnose debug flow filter negate port on page 2781](#)
- [diagnose debug flow filter negate proto on page 2782](#)
- [diagnose debug flow filter negate saddr on page 2782](#)
- [diagnose debug flow filter negate sport on page 2782](#)
- [diagnose debug flow filter negate vd on page 2782](#)
- [diagnose debug flow filter port on page 2782](#)
- [diagnose debug flow filter proto on page 2782](#)
- [diagnose debug flow filter saddr on page 2783](#)
- [diagnose debug flow filter sport on page 2783](#)
- [diagnose debug flow filter vd on page 2783](#)
- [diagnose debug flow filter vd-name on page 2783](#)
- [diagnose debug flow filter6 on page 2784](#)
- [diagnose debug flow filter6 addr on page 2784](#)
- [diagnose debug flow filter6 clear on page 2784](#)
- [diagnose debug flow filter6 daddr on page 2784](#)
- [diagnose debug flow filter6 dport on page 2785](#)
- [diagnose debug flow filter6 negate on page 2785](#)
- [diagnose debug flow filter6 negate addr on page 2785](#)
- [diagnose debug flow filter6 negate daddr on page 2785](#)
- [diagnose debug flow filter6 negate dport on page 2785](#)
- [diagnose debug flow filter6 negate port on page 2785](#)
- [diagnose debug flow filter6 negate proto on page 2786](#)
- [diagnose debug flow filter6 negate saddr on page 2786](#)
- [diagnose debug flow filter6 negate sport on page 2786](#)
- [diagnose debug flow filter6 negate vd on page 2786](#)
- [diagnose debug flow filter6 port on page 2786](#)
- [diagnose debug flow filter6 proto on page 2786](#)
- [diagnose debug flow filter6 saddr on page 2787](#)

- [diagnose debug flow filter6 sport on page 2787](#)
- [diagnose debug flow filter6 vd on page 2787](#)
- [diagnose debug flow filter6 vd-name on page 2787](#)
- [diagnose debug flow show on page 2788](#)
- [diagnose debug flow show function-name on page 2788](#)
- [diagnose debug flow show function-name disable on page 2788](#)
- [diagnose debug flow show function-name enable on page 2788](#)
- [diagnose debug flow show iprope on page 2788](#)
- [diagnose debug flow show iprope disable on page 2788](#)
- [diagnose debug flow show iprope enable on page 2789](#)
- [diagnose debug flow trace on page 2789](#)
- [diagnose debug flow trace start on page 2789](#)
- [diagnose debug flow trace start6 on page 2789](#)
- [diagnose debug flow trace stop on page 2789](#)
- [diagnose debug flow trace stop6 on page 2790](#)
- [diagnose debug fortalink-report on page 2790](#)
- [diagnose debug fortalink-report all on page 2790](#)
- [diagnose debug fortalink-report switch-group on page 2790](#)
- [diagnose debug fortalink-report switch-id on page 2790](#)
- [diagnose debug fortism on page 2791](#)
- [diagnose debug fortism enable on page 2791](#)
- [diagnose debug fsso-polling on page 2791](#)
- [diagnose debug fsso-polling client on page 2791](#)
- [diagnose debug fsso-polling detail on page 2791](#)
- [diagnose debug fsso-polling group on page 2791](#)
- [diagnose debug fsso-polling refresh-user on page 2792](#)
- [diagnose debug fsso-polling set-log-source on page 2792](#)
- [diagnose debug fsso-polling summary on page 2792](#)
- [diagnose debug fsso-polling user on page 2792](#)
- [diagnose debug info on page 2793](#)
- [diagnose debug kernel on page 2793](#)
- [diagnose debug kernel ha on page 2793](#)
- [diagnose debug kernel level on page 2793](#)
- [diagnose debug kernel sysrq on page 2793](#)
- [diagnose debug kernel sysrq command on page 2794](#)
- [diagnose debug kernel sysrq command crash on page 2794](#)
- [diagnose debug kernel sysrq disable on page 2794](#)
- [diagnose debug kernel sysrq enable on page 2794](#)
- [diagnose debug kernel sysrq status on page 2794](#)
- [diagnose debug rating on page 2794](#)
- [diagnose debug report on page 2795](#)
- [diagnose debug report reset on page 2795](#)
- [diagnose debug reset on page 2795](#)

- [diagnose debug sdnc on page 2795](#)
- [diagnose debug sdnc valgrind on page 2795](#)
- [diagnose debug sdnc valgrind disable on page 2795](#)
- [diagnose debug sdnc valgrind enable on page 2796](#)
- [diagnose debug sdnc valgrind log on page 2796](#)
- [diagnose debug sdnc valgrind log clear on page 2796](#)
- [diagnose debug sdnc valgrind log show on page 2796](#)
- [diagnose debug sdnc valgrind memcheck on page 2796](#)
- [diagnose debug sdnc valgrind memcheck_less on page 2796](#)
- [diagnose debug sdnc valgrind status on page 2797](#)
- [diagnose debug sql-log-error on page 2797](#)
- [diagnose debug sql-log-error clear on page 2797](#)
- [diagnose debug sql-log-error read on page 2797](#)
- [diagnose debug sql-log-error status on page 2797](#)
- [diagnose debug traffic on page 2797](#)
- [diagnose debug traffic dump-debug on page 2798](#)
- [diagnose debug traffic error on page 2798](#)
- [diagnose debug traffic history on page 2798](#)
- [diagnose debug traffic interface on page 2798](#)
- [diagnose debug traffic peek on page 2798](#)
- [diagnose debug urlfilter on page 2799](#)
- [diagnose debug urlfilter src-addr on page 2799](#)
- [diagnose debug urlfilter test-url on page 2799](#)
- [diagnose debug urlfilter valgrind on page 2799](#)
- [diagnose debug urlfilter valgrind disable on page 2799](#)
- [diagnose debug urlfilter valgrind enable on page 2800](#)
- [diagnose debug urlfilter valgrind log on page 2800](#)
- [diagnose debug urlfilter valgrind log clear on page 2800](#)
- [diagnose debug urlfilter valgrind log show on page 2800](#)
- [diagnose debug urlfilter valgrind memcheck on page 2800](#)
- [diagnose debug urlfilter valgrind memcheck_less on page 2800](#)
- [diagnose debug urlfilter valgrind status on page 2801](#)
- [diagnose debug user on page 2801](#)
- [diagnose debug user hash on page 2801](#)
- [diagnose debug user list on page 2801](#)
- [diagnose debug vm-print-license on page 2801](#)
- [diagnose debug vpce on page 2801](#)

diagnose debug admin

Admin user.

```
diagnose debug admin
```

diagnose debug admin error-log

Last failed admin user login details.

```
diagnose debug admin error-log
```

diagnose debug application

application

```
diagnose debug application
```

diagnose debug application acd

Aggregate Controller

```
diagnose debug application acd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application acid

Cisco Application Centric Infrastructure (Direct Connection) daemon

```
diagnose debug application acid <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application alarmd

Alarmd daemon.

```
diagnose debug application alarmd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application alertmail

Alert mail daemon.

```
diagnose debug application alertmail <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application alicloud-ha

AliCloud HA controller

```
diagnose debug application alicloud-ha <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application alicloud-sdn

AliCloud SDN controller

```
diagnose debug application alicloud-sdn <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application authd

Auth daemon.

```
diagnose debug application authd <Integer> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	
<xxx.xxx.xxx.xxx>	Specific source IP to debug some modules (e.g.fsso).	string	

diagnose debug application autod

Automation daemon.

```
diagnose debug application autod <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application awsd

Amazon Web Services (AWS) daemon.

```
diagnose debug application awsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application azd

Microsoft Azure daemon.

```
diagnose debug application azd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application azd-ha

Microsoft Azure daemon.

```
diagnose debug application azd-ha <Integer>
```


Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application bfdd

BFD daemon.

```
diagnose debug application bfdd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application cert-update

Certificate update in forticron daemon.

```
diagnose debug application cert-update <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application chassis

Chassis daemon.

```
diagnose debug application chassis <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application clearpass

ClearPass daemon.

```
diagnose debug application clearpass <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application cloudapid

Cloud service communication daemon.

```
diagnose debug application cloudapid <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application cloudinitd

cloudinitd daemon.

```
diagnose debug application cloudinitd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application cmp

CMPv2.

```
diagnose debug application cmp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application crl-update

CRL update in forticron daemon.

```
diagnose debug application crl-update <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application csfd

Security Fabric daemon.

```
diagnose debug application csfd <Integer> <serial <serialnum>|ip <ip>|direction <up|down>> <serial  
<serialnum>|ip <ip>|direction <up|down>> <enter>|negate
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	
<serial <serialnum> ip <ip> direction <up down>>	Filter by serial number, IP, or stream direction.	string	
<serial <serialnum> ip <ip> direction <up down>>	Filter by serial number, IP, or stream direction.	string	
<enter> negate	If negate, inverse filter.	string	

diagnose debug application cu_acd

caputp AC daemon

```
diagnose debug application cu_acd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application cw_acd

Capwap AC daemon.

```
diagnose debug application cw_acd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application cw_acd_helper

Capwap AC helper daemon.

```
diagnose debug application cw_acd_helper <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application cw_acd_wlev

CAPWAP AC daemon wireless event notification.

```
diagnose debug application cw_acd_wlev <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application cw_acd_wpad

CAPWAP AC and WPA daemon (wpad).

```
diagnose debug application cw_acd_wpad <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ddnsd

DDNS client daemon.

```
diagnose debug application ddnsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dhcp6c

DHCPv6 client.

```
diagnose debug application dhcp6c <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dhcp6r

DHCPv6 relay.

```
diagnose debug application dhcp6r <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dhcp6s

DHCPv6 server.

```
diagnose debug application dhcp6s <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dhcpc

DHCP client module.

```
diagnose debug application dhcpc <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dhcprelay

DHCP relay daemon.

```
diagnose debug application dhcprelay <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dhcps

DHCP server.

```
diagnose debug application dhcps <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dlpfingerprint

DLP fingerprint daemon.

```
diagnose debug application dlpfingerprint <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dnp

DNP proxy daemon.

```
diagnose debug application dnp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application dnsproxy

DNS proxy module.

```
diagnose debug application dnsproxy <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	
<Integer>	Daemon index.	string	

diagnose debug application eap_proxy

EAP proxy daemon.

```
diagnose debug application eap_proxy <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application eap_supp

EAP supplicant daemon.

```
diagnose debug application eap_supp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application est

Enrollment over Secure Transport

```
diagnose debug application est <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application evpnd

EVPN daemon.

```
diagnose debug application evpnd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application extenderd

Extender Wan daemon.

```
diagnose debug application extenderd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fclfd

Fclfd daemon.

```
diagnose debug application fclfd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fcnacd

FortiClient NAC daemon.

```
diagnose debug application fcnacd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fds_notify

Update notification daemon.

```
diagnose debug application fds_notify <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fgd_alert

FortiGuard alert message.

```
diagnose debug application fgd_alert <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fgfmd

FortiGate/FortiManager communication daemon.


```
diagnose debug application fgfmd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fgtlogd

fgtlogd daemon.

```
diagnose debug application fgtlogd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application flcfgd

fortilink configuration daemon

```
diagnose debug application flcfgd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application flpold

FortiLink policy daemon.

```
diagnose debug application flpold <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fltund

FortiLink tunnel daemon.

```
diagnose debug application fltund <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fnbamd

FortiGate non-blocking auth daemon.

```
diagnose debug application fnbamd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application foauthd

FortiGuardOverride auth daemon.

```
diagnose debug application foauthd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application forticldd

FortiCloud daemon.

```
diagnose debug application forticldd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application forticron

Forticron daemon.

```
diagnose debug application forticron <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fortinkd

fortinkd daemon

```
diagnose debug application fortinkd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fortimq

Fortimq daemon.

```
diagnose debug application fortimq <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fsso_ldap

FSSO LDAP daemon.

```
diagnose debug application fsso_ldap <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fssod

FSSO daemon.

```
diagnose debug application fssod <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application fsvrd

FortiService daemon.

```
diagnose debug application fsvrd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ftm-push

FTM-Push daemon.

```
diagnose debug application ftm-push <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application garpd

VIP gratuitous ARP daemon.

```
diagnose debug application garpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application gcpd

Google Cloud Platform daemon.

```
diagnose debug application gcpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application hamonitord

HA monitor module.

```
diagnose debug application hamonitord <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application harelay

HA relay module.

```
diagnose debug application harelay <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application hasync

HA synchronization module.

```
diagnose debug application hasync <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application hatalk

HA protocol module.

```
diagnose debug application hatalk <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application httpsd

HTTPS daemon.

```
diagnose debug application httpsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level. (Info = 0x01, Warning = 0x02, Error = 0x04, Critical = 0x08, All = -1, Warning/Error/Critical = 0x0E)	string	

diagnose debug application ibmd

IBM Cloud Infrastructure daemon.

```
diagnose debug application ibmd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application icond

Industrial Connectivity daemon.

```
diagnose debug application icond <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ike

IKE daemon.

```
diagnose debug application ike <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ikecrypt

Multi-process IKE crypto daemon.

```
diagnose debug application ikecrypt <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application imap

IMAP proxy.

```
diagnose debug application imap <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application init

System init process.

```
diagnose debug application init <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application iotd

IoT device info daemon.

```
diagnose debug application iotd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ipamd

IP Address Management daemon.

```
diagnose debug application ipamd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ipamsd

IPAM server daemon.

```
diagnose debug application ipamsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ipldbd

Ipldbd daemon.

```
diagnose debug application ipldbd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ipsengine

IPS sensor.

```
diagnose debug application ipsengine <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ipsmonitor

IPS monitor.

```
diagnose debug application ipsmonitor <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ipsufd

IPS URL filter resolver daemon.


```
diagnose debug application ipsufd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application kmiglogd

Kernel Log daemon.

```
diagnose debug application kmiglogd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application kmipd

KMIP daemon

```
diagnose debug application kmipd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application kubed

Kubernetes daemon.

```
diagnose debug application kubed <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application l2tp

L2TP daemon.

```
diagnose debug application l2tp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application link-monitor

Link monitor daemon.

```
diagnose debug application link-monitor <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application link-monitor-passive

Link monitor daemon.

```
diagnose debug application link-monitor-passive <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application locallogd

locallogd daemon.

```
diagnose debug application locallogd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application lpmd

LPM daemon.

```
diagnose debug application lpmd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application miglogd

Log daemon.

```
diagnose debug application miglogd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application mrd

Mobile router daemon.

```
diagnose debug application mrd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application netxd

NetX REST API daemon.

```
diagnose debug application netxd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application nntp

NNTP proxy.

```
diagnose debug application nntp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application nodejs

Node.js daemon.

```
diagnose debug application nodejs <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level. (Info = 0x01, Warning = 0x02, Error = 0x04, All = -1, Warning/Error = 0x06)	string	

diagnose debug application npd

NP7 daemon.

```
diagnose debug application npd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ntnxd

Nutanix Prism Central daemon.

```
diagnose debug application ntnxd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ntpd

NTPd daemon.

```
diagnose debug application ntpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application oaas_agent

OaaS agent daemon.

```
diagnose debug application oaas_agent <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ocid

Oracle Cloud Infrastructure (OCI) daemon

```
diagnose debug application ocid <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application openstackd

OpenStack SDN connector daemon.

```
diagnose debug application openstackd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ovrd

Override daemon.

```
diagnose debug application ovrd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application pcpd

PCP server daemon.

```
diagnose debug application pcpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application pop3

POP3 proxy.

```
diagnose debug application pop3 <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ppp

PPP daemon.

```
diagnose debug application ppp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application pppoe

PPPoE client Daemon.

```
diagnose debug application pppoe <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application pptp

PPTP daemon.

```
diagnose debug application pptp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application pptpc

PPTP client.

```
diagnose debug application pptpc <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application proxy

Proxy.

```
diagnose debug application proxy <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application ptpd

Precision Time Protocol daemon.

```
diagnose debug application ptpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application quarantine

Quarantine daemon.

```
diagnose debug application quarantine <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application radius-das

RADIUS DAS daemon.

```
diagnose debug application radius-das <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application radiusd

RADIUS daemon.

```
diagnose debug application radiusd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application radvd

Router adv daemon.

```
diagnose debug application radvd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application reportd

report daemon

```
diagnose debug application reportd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application route-tag

route-tag daemon.

```
diagnose debug application route-tag <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application samld

SAML SSO daemon.

```
diagnose debug application samld <Integer> <verbose>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	
<verbose>	Verbose output during process. (v, vv, vvv)	string	

diagnose debug application sapd

SAP Control daemon.

```
diagnose debug application sapd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sccp

SCCP ALG.

```
diagnose debug application sccp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application scep

SCEP

```
diagnose debug application scep <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application scimd

SCIM server daemon.

```
diagnose debug application scimd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sdncd

SDN Connector daemon.

```
diagnose debug application sdncd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sdnvpnd

Public Cloud VPN daemon.

```
diagnose debug application sdnvpnd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sdwan

SD-WAN daemon.

```
diagnose debug application sdwan <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sepmd

Symantec EPM daemon.

```
diagnose debug application sepmd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application server-probe

Server probe daemon.

```
diagnose debug application server-probe <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sessionsync

Session sync daemon.

```
diagnose debug application sessionsync <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sflowd

sFlow protocol module.

```
diagnose debug application sflowd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sfupgraded

Security Fabric Upgrade daemon.

```
diagnose debug application sfupgraded <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sip

SIP ALG.

```
diagnose debug application sip <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application smbcd

SMB client daemon.

```
diagnose debug application smbcd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application smtp

SMTP proxy.

```
diagnose debug application smtp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application snmpd

SNMP daemon.

```
diagnose debug application snmpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application spareblock

Set debug spare block count.

```
diagnose debug application spareblock <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application speedtest

Speed test execution daemon.

```
diagnose debug application speedtest <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application speedtestd

Speed test server daemon.

```
diagnose debug application speedtestd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sshd

Sshd daemon.

```
diagnose debug application sshd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application sslvpn

Agentless VPN proxy daemon

```
diagnose debug application sslvpn <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application syslogd

syslogd daemon.

```
diagnose debug application syslogd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application update

Update daemon.

```
diagnose debug application update <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application uploadd

Upload daemon.

```
diagnose debug application uploadd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application urlfilter

Urlfilter daemon.

```
diagnose debug application urlfilter <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application vmwd

VMware vSphere daemon

```
diagnose debug application vmwd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application vned

Virtual network enabler daemon.

```
diagnose debug application vned <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application vrrpd

VRRP daemon.

```
diagnose debug application vrrpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application wabcs

WAN acceleration byte cache storage.

```
diagnose debug application wabcs <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application waocs

WAN acceleration object cache storage.

```
diagnose debug application waocs <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application wccpd

WCCP daemon.

```
diagnose debug application wccpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application wf_monitor

WF monitor, parent of urlfilter daemon.

```
diagnose debug application wf_monitor <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application wifi

WiFi setting.

```
diagnose debug application wifi <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application wpa-show-keys

Dump keys in wpad or wpas log.


```
diagnose debug application wpa-show-keys <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application wpa-timestamp

Dump timestamp in wpad or wpas log.

```
diagnose debug application wpa-timestamp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application wpad

Port access entity daemon.

```
diagnose debug application wpad <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application wpad-crash-hexdump

Dump wpad crash in hexadecimal format.

```
diagnose debug application wpad-crash-hexdump <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application zebos

ZebOS

```
diagnose debug application zebos <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application zebos-launcher

ZebOS launcher daemon.

```
diagnose debug application zebos-launcher <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug authd

Authentication daemon.

```
diagnose debug authd
```

diagnose debug authd clear

Clear internal data structures and keep alive sessions.

```
diagnose debug authd clear
```

diagnose debug authd fsso

FSSO client module.

```
diagnose debug authd fsso
```

diagnose debug authd fsso add-address

Add FSAE dynamic addresses.

```
diagnose debug authd fsso add-address <adgrp1+adgrp2+...*adgrpn> <xxx.xxx.xxx.xxx>  
<xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<adgrp1+adgrp2+...*adgrpn>	AD groups.	string	
<xxx.xxx.xxx.xxx>	IP start address.	string	
<xxx.xxx.xxx.xxx>	IP end address.	string	

diagnose debug authd fsso clear-logons

Clear logon information.

```
diagnose debug authd fsso clear-logons
```

diagnose debug authd fsso del-address

Delete FSAE dynamic addresses.

```
diagnose debug authd fsso del-address <adgrp1+adgrp2+...*adgrpn> <xxx.xxx.xxx.xxx>  
<xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<adgrp1+adgrp2+...*adgrpn>	AD groups.	string	
<xxx.xxx.xxx.xxx>	IP start address.	string	
<xxx.xxx.xxx.xxx>	IP end address.	string	

diagnose debug authd fsso filter

Filters used for list or clear logons.

```
diagnose debug authd fsso filter
```

diagnose debug authd fsso filter clear

Clear all filters.

```
diagnose debug authd fsso filter clear
```

diagnose debug authd fsso filter group

Group name.

```
diagnose debug authd fsso filter group <name>
```

Parameter	Description	Type	Size
<name>	Group name.	string	

diagnose debug authd fsso filter server

FSSO agent name.

```
diagnose debug authd fsso filter server <name>
```

Parameter	Description	Type	Size
<name>	FSSO agent name.	string	

diagnose debug authd fsso filter source

Source IP address.

```
diagnose debug authd fsso filter source <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (range from).	string	
<xxx.xxx.xxx.xxx>	Source IP (range to).	string	

diagnose debug authd fsso filter user

User name.

```
diagnose debug authd fsso filter user <name>
```

Parameter	Description	Type	Size
<name>	User name.	string	

diagnose debug authd fsso flush-address

Flush FSAE dynamic addresse.

```
diagnose debug authd fsso flush-address <name>
```

Parameter	Description	Type	Size
<name>	FSSO address name.	string	

diagnose debug authd fsso flush-address-all

Flush all of FSAE dynamic addresses.

```
diagnose debug authd fsso flush-address-all
```

diagnose debug authd fsso list

List current logons.

```
diagnose debug authd fsso list
```

diagnose debug authd fsso refresh-groups

Refresh group mappings.

```
diagnose debug authd fsso refresh-groups
```

diagnose debug authd fsso refresh-logons

Resync logon database.

```
diagnose debug authd fsso refresh-logons
```

diagnose debug authd fsso server-status

Show FSSO agent connection status.

```
diagnose debug authd fsso server-status
```

diagnose debug authd fsso show-address

Show FSAE dynamic addresses.

```
diagnose debug authd fsso show-address
```

diagnose debug authd fsso summary

Summary of current logons.

```
diagnose debug authd fsso summary
```

diagnose debug authd memory

Show authd memory usage information.

```
diagnose debug authd memory
```

diagnose debug aws-vpce

Print kernel aws vpce info.

```
diagnose debug aws-vpce
```

diagnose debug backtrace

Generate backtrace with <type>

```
diagnose debug backtrace
```

diagnose debug cli

Debug CLI.

```
diagnose debug cli <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level (0 - 8).	string	

diagnose debug cloudinit

Cloudinit info.

```
diagnose debug cloudinit
```

diagnose debug cloudinit clear

Clear cloudinit log info.

```
diagnose debug cloudinit clear
```

diagnose debug cloudinit show

Show cloudinit log info.

```
diagnose debug cloudinit show
```

diagnose debug cmdb-trace

Trace CLI.

```
diagnose debug cmdb-trace <Integer>
```

Parameter	Description	Type	Size
<Integer>	Trace level (0 - 2).	string	

diagnose debug cmdb-walk

enable/disable cmdb-walk.

```
diagnose debug cmdb-walk <Integer>
```

Parameter	Description	Type	Size
<Integer>	walk value (0 - 1).	string	

diagnose debug config-error-log

Configure error log info.

```
diagnose debug config-error-log
```

diagnose debug config-error-log clear

Clear config error log.

```
diagnose debug config-error-log clear
```

diagnose debug config-error-log read

Display config error on console.

```
diagnose debug config-error-log read
```

diagnose debug console

console

```
diagnose debug console
```

diagnose debug console no-user-log-msg

Console does not show user log messages.

```
diagnose debug console no-user-log-msg
```

diagnose debug console no-user-log-msg disable

Disable console no user log message.

```
diagnose debug console no-user-log-msg disable
```


diagnose debug console no-user-log-msg enable

Enable console no user log message.

```
diagnose debug console no-user-log-msg enable
```

diagnose debug console retry-log-msg

Console does not drop user log messages.

```
diagnose debug console retry-log-msg
```

diagnose debug console retry-log-msg disable

Disable console resend of user log message.

```
diagnose debug console retry-log-msg disable
```

diagnose debug console retry-log-msg enable

Enable console resend of user log message.

```
diagnose debug console retry-log-msg enable
```

diagnose debug console send

Send out MODEM AT command.

```
diagnose debug console send <AT command> <character> <integer>
```

Parameter	Description	Type	Size
<AT command>	MODEM AT command to send.	string	
<character>	escape character (optional, default is '+')	string	
<integer>	Escape guard time in milli-second (1 - 10000, optional, default = 1000ms).	string	

diagnose debug console timestamp

timestamp

```
diagnose debug console timestamp
```

diagnose debug console timestamp disable

Disable timestamp.

```
diagnose debug console timestamp disable
```

diagnose debug console timestamp enable

Enable timestamp.

```
diagnose debug console timestamp enable
```

diagnose debug crashlog

Crash log info.

```
diagnose debug crashlog
```

diagnose debug crashlog clear

Clear crash log.

```
diagnose debug crashlog clear
```

diagnose debug crashlog get

Get crashlog.

```
diagnose debug crashlog get
```

diagnose debug crashlog history

Show process crash history.

```
diagnose debug crashlog history
```

diagnose debug crashlog interval

Change crash log interval in seconds.

```
diagnose debug crashlog interval <interval>
```

Parameter	Description	Type	Size
<interval>	Interval at which process crashes are written to storage (0 - 2147483647 sec, default = 3600, 0 = log all crashes).	string	

diagnose debug disable

Disable debug output.

```
diagnose debug disable
```

diagnose debug duration

Set duration of debug activities.

```
diagnose debug duration <Integer>
```

Parameter	Description	Type	Size
<Integer>	Duration in minutes, min = 1, max = 99999, 0 means unlimited.	string	

diagnose debug enable

Enable debug output.

```
diagnose debug enable
```

diagnose debug flow

Trace packet flow in kernel.

```
diagnose debug flow
```

diagnose debug flow filter

Trace packet with filter.

```
diagnose debug flow filter
```

diagnose debug flow filter addr

IP address.

```
diagnose debug flow filter addr <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx> <Enter> | or/and
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Host IP (ip1/from).	string	
<xxx.xxx.xxx.xxx>	Host IP (ip2/to).	string	
<Enter> or/and	If or/and is specific, filter base on ip1 or/and ip2.	string	

diagnose debug flow filter clear

Clear filter.

```
diagnose debug flow filter clear
```

diagnose debug flow filter daddr

Destination IP address.

```
diagnose debug flow filter daddr <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP (from).	string	
<xxx.xxx.xxx.xxx>	Destination IP (to).	string	

diagnose debug flow filter dport

Destination port.

```
diagnose debug flow filter dport <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Destination port (from).	string	
<xxx>	Destination port (to).	string	

diagnose debug flow filter negate

Inverse filter.

```
diagnose debug flow filter negate
```

diagnose debug flow filter negate addr

Inverse host IP.

```
diagnose debug flow filter negate addr
```

diagnose debug flow filter negate daddr

Inverse dest IP.

```
diagnose debug flow filter negate daddr
```

diagnose debug flow filter negate dport

Inverse dest port.

```
diagnose debug flow filter negate dport
```

diagnose debug flow filter negate port

Inverse port.

```
diagnose debug flow filter negate port
```

diagnose debug flow filter negate proto

Inverse protocol.

```
diagnose debug flow filter negate proto
```

diagnose debug flow filter negate saddr

Inverse source IP.

```
diagnose debug flow filter negate saddr
```

diagnose debug flow filter negate sport

Inverse source port.

```
diagnose debug flow filter negate sport
```

diagnose debug flow filter negate vd

Inverse virtual domain.

```
diagnose debug flow filter negate vd
```

diagnose debug flow filter port

port

```
diagnose debug flow filter port <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Port (from).	string	
<xxx>	Port (to).	string	

diagnose debug flow filter proto

Protocol number.

```
diagnose debug flow filter proto <xxx>
```

Parameter	Description	Type	Size
<xxx>	Protocol number.	string	

diagnose debug flow filter saddr

Source IP address.

```
diagnose debug flow filter saddr <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (from).	string	
<xxx.xxx.xxx.xxx>	Source IP (to).	string	

diagnose debug flow filter sport

Source port.

```
diagnose debug flow filter sport <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Source port (from).	string	
<xxx>	Source port (to).	string	

diagnose debug flow filter vd

Index of virtual domain.

```
diagnose debug flow filter vd <xxx>
```

Parameter	Description	Type	Size
<xxx>	Index of virtual domain.	string	

diagnose debug flow filter vd-name

Name of virtual domain.

```
diagnose debug flow filter vd-name <...>
```

Parameter	Description	Type	Size
<...>	Name of virtual domain.	string	

diagnose debug flow filter6

Trace packet with IPv6 filter.

```
diagnose debug flow filter6
```

diagnose debug flow filter6 addr

IPv6 address.

```
diagnose debug flow filter6 addr <xxx:xxx::xxx:xxx> <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Host IPv6 (from).	string	
<xxx:xxx::xxx:xxx>	Host IPv6 (to).	string	

diagnose debug flow filter6 clear

Clear IPv6 filter.

```
diagnose debug flow filter6 clear
```

diagnose debug flow filter6 daddr

Destination IP address.

```
diagnose debug flow filter6 daddr <xxx:xxx::xxx:xxx> <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Destination IP (from).	string	
<xxx:xxx::xxx:xxx>	Destination IP (to).	string	

diagnose debug flow filter6 dport

Destination port.

```
diagnose debug flow filter6 dport <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Destination port (from).	string	
<xxx>	Destination port (to).	string	

diagnose debug flow filter6 negate

Inverse IPv6 filter.

```
diagnose debug flow filter6 negate
```

diagnose debug flow filter6 negate addr

Inverse host IP.

```
diagnose debug flow filter6 negate addr
```

diagnose debug flow filter6 negate daddr

Inverse dest IP.

```
diagnose debug flow filter6 negate daddr
```

diagnose debug flow filter6 negate dport

Inverse dest port.

```
diagnose debug flow filter6 negate dport
```

diagnose debug flow filter6 negate port

Inverse port.

```
diagnose debug flow filter6 negate port
```

diagnose debug flow filter6 negate proto

Inverse protocol.

```
diagnose debug flow filter6 negate proto
```

diagnose debug flow filter6 negate saddr

Inverse source IP.

```
diagnose debug flow filter6 negate saddr
```

diagnose debug flow filter6 negate sport

Inverse source port.

```
diagnose debug flow filter6 negate sport
```

diagnose debug flow filter6 negate vd

Inverse virtual domain.

```
diagnose debug flow filter6 negate vd
```

diagnose debug flow filter6 port

port

```
diagnose debug flow filter6 port <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Port (from).	string	
<xxx>	Port (to).	string	

diagnose debug flow filter6 proto

Protocol number.

```
diagnose debug flow filter6 proto <xxx>
```

Parameter	Description	Type	Size
<xxx>	Protocol number.	string	

diagnose debug flow filter6 saddr

Source IP address.

```
diagnose debug flow filter6 saddr <xxx:xxx::xxx:xxx> <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Source IP (from).	string	
<xxx:xxx::xxx:xxx>	Source IP (to).	string	

diagnose debug flow filter6 sport

Source port.

```
diagnose debug flow filter6 sport <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Source port (from).	string	
<xxx>	Source port (to).	string	

diagnose debug flow filter6 vd

Index of virtual domain.

```
diagnose debug flow filter6 vd <xxx>
```

Parameter	Description	Type	Size
<xxx>	Index of virtual domain.	string	

diagnose debug flow filter6 vd-name

Name of virtual domain.

```
diagnose debug flow filter6 vd-name <...>
```

Parameter	Description	Type	Size
<...>	Name of virtual domain.	string	

diagnose debug flow show

Enable/disable display of trace on console.

```
diagnose debug flow show
```

diagnose debug flow show function-name

Enable/disable display function name.

```
diagnose debug flow show function-name
```

diagnose debug flow show function-name disable

Disable display of function name.

```
diagnose debug flow show function-name disable
```

diagnose debug flow show function-name enable

Enable display of function name.

```
diagnose debug flow show function-name enable
```

diagnose debug flow show iprope

Enable/disable trace iprope match.

```
diagnose debug flow show iprope
```

diagnose debug flow show iprope disable

Disable trace iprope match.

```
diagnose debug flow show iprope disable
```

diagnose debug flow show iprope enable

Enable trace iprope match.

```
diagnose debug flow show iprope enable
```

diagnose debug flow trace

Start/stop trace.

```
diagnose debug flow trace
```

diagnose debug flow trace start

Start trace.

```
diagnose debug flow trace start <xxx>
```

Parameter	Description	Type	Size
<xxx>	Repeat number.	string	

diagnose debug flow trace start6

Start IPv6 trace.

```
diagnose debug flow trace start6 <xxx>
```

Parameter	Description	Type	Size
<xxx>	Repeat number.	string	

diagnose debug flow trace stop

Stop trace.

```
diagnose debug flow trace stop
```

diagnose debug flow trace stop6

Stop IPv6 trace.

```
diagnose debug flow trace stop6
```

diagnose debug fortilink-report

Generate FortiLink debug report.

```
diagnose debug fortilink-report
```

diagnose debug fortilink-report all

Generate FortiLink debug report for all switches.

```
diagnose debug fortilink-report all
```

diagnose debug fortilink-report switch-group

Generate FortiLink debug report for switch group.

```
diagnose debug fortilink-report switch-group <switch-group>
```

Parameter	Description	Type	Size
<switch-group>	Switch group name.	string	

diagnose debug fortilink-report switch-id

Generate FortiLink debug report for switch by specific switch ID.

```
diagnose debug fortilink-report switch-id <switch-id>
```

Parameter	Description	Type	Size
<switch-id>	Switch ID.	string	

diagnose debug fortism

Fortinet security module.

```
diagnose debug fortism
```

diagnose debug fortism enable

Enable Fortinet security module for test purpose.

```
diagnose debug fortism enable
```

diagnose debug fsso-polling

FSSO active directory poll module.

```
diagnose debug fsso-polling
```

diagnose debug fsso-polling client

Show FSSO AD Server Clients.

```
diagnose debug fsso-polling client
```

diagnose debug fsso-polling detail

Show FSSO AD Server Detail.

```
diagnose debug fsso-polling detail <id>
```

Parameter	Description	Type	Size
<id>	AD Server Entry ID.	string	

diagnose debug fsso-polling group

Show FSSO LDAP groups for AD users.

```
diagnose debug fsso-polling group <id> <name>
```

Parameter	Description	Type	Size
<id>	AD Server Entry ID.	string	
<name>	AD Server user.	string	

diagnose debug fsso-polling refresh-user

Refresh FSSO AD Server users.

```
diagnose debug fsso-polling refresh-user <id>
```

Parameter	Description	Type	Size
<id>	AD Server Entry ID.	string	

diagnose debug fsso-polling set-log-source

Source of event log.

```
diagnose debug fsso-polling set-log-source <id> <src>
```

Parameter	Description	Type	Size
<id>	AD Server Entry ID.	string	
<src>	0: security, 1:application.	string	

diagnose debug fsso-polling summary

Show FSSO AD Server Summary.

```
diagnose debug fsso-polling summary
```

diagnose debug fsso-polling user

Show FSSO AD Server users.

```
diagnose debug fsso-polling user <id>
```

Parameter	Description	Type	Size
<id>	AD Server Entry ID.	string	

diagnose debug info

Show active debug level settings.

```
diagnose debug info
```

diagnose debug kernel

kernel

```
diagnose debug kernel
```

diagnose debug kernel ha

Debug kernel HA level.

```
diagnose debug kernel ha <Integer>
```

Parameter	Description	Type	Size
<Integer>	Kernel HA level (0 = disable, 1-7 = higher level).	string	

diagnose debug kernel level

Debug kernel level.

```
diagnose debug kernel level <Integer>
```

Parameter	Description	Type	Size
<Integer>	Kernel level.	string	

diagnose debug kernel sysrq

Magic SysRq.

```
diagnose debug kernel sysrq
```

diagnose debug kernel sysrq command

Magic SysRq command.

```
diagnose debug kernel sysrq command
```

diagnose debug kernel sysrq command crash

Perform a system crash.

```
diagnose debug kernel sysrq command crash
```

diagnose debug kernel sysrq disable

Disable magic SysRq.

```
diagnose debug kernel sysrq disable
```

diagnose debug kernel sysrq enable

Enable magic SysRq.

```
diagnose debug kernel sysrq enable
```

diagnose debug kernel sysrq status

Show the status of magic SysRq.

```
diagnose debug kernel sysrq status
```

diagnose debug rating

Display rating info.

```
diagnose debug rating <refresh-rate>
```

Parameter	Description	Type	Size
<refresh-rate>	Frequency to refresh server list (sec).	string	

diagnose debug report

Report for tech support.

```
diagnose debug report
```

diagnose debug report reset

Reset debug report.

```
diagnose debug report reset
```

diagnose debug reset

Reset all debug level to default.

```
diagnose debug reset
```

diagnose debug sdnc

sdnc

```
diagnose debug sdnc
```

diagnose debug sdnc valgrind

Valgrind analysis.

```
diagnose debug sdnc valgrind
```

diagnose debug sdnc valgrind disable

Force daemon to restart.

```
diagnose debug sdnc valgrind disable
```

diagnose debug sdnc valgrind enable

Force daemon to restart.

```
diagnose debug sdnc valgrind enable
```

diagnose debug sdnc valgrind log

Valgrind logs.

```
diagnose debug sdnc valgrind log
```

diagnose debug sdnc valgrind log clear

Clear logs.

```
diagnose debug sdnc valgrind log clear
```

diagnose debug sdnc valgrind log show

Show logs.

```
diagnose debug sdnc valgrind log show
```

diagnose debug sdnc valgrind memcheck

Force daemon to restart.

```
diagnose debug sdnc valgrind memcheck
```

diagnose debug sdnc valgrind memcheck_less

Force daemon to restart.

```
diagnose debug sdnc valgrind memcheck_less
```

diagnose debug sdnc valgrind status

Show valgrind status.

```
diagnose debug sdnc valgrind status
```

diagnose debug sql-log-error

SQL log database error info

```
diagnose debug sql-log-error
```

diagnose debug sql-log-error clear

clear sql log database error log

```
diagnose debug sql-log-error clear
```

diagnose debug sql-log-error read

display sql log database error on console

```
diagnose debug sql-log-error read
```

diagnose debug sql-log-error status

show sql log database error status

```
diagnose debug sql-log-error status
```

diagnose debug traffic

Traffic statistic data

```
diagnose debug traffic
```

diagnose debug traffic dump-debug

Dump debug info for interface traffic history.

```
diagnose debug traffic dump-debug
```

diagnose debug traffic error

Show error counter of interface bandwidth.

```
diagnose debug traffic error
```

diagnose debug traffic history

Dump interface traffic history data.

```
diagnose debug traffic history <String> <Integer>
```

Parameter	Description	Type	Size
<String>	Interface name	string	
<Integer>	Period, hour=0, day=1, week=2.	string	

diagnose debug traffic interface

List traffic monitor interface.

```
diagnose debug traffic interface
```

diagnose debug traffic peek

Display interface traffic real-time data.

```
diagnose debug traffic peek <String> <Integer>
```

Parameter	Description	Type	Size
<String>	Interface name	string	
<Integer>	Disable or enable, disable=0, enable=1.	string	

diagnose debug urlfilter

urlfilter

```
diagnose debug urlfilter
```

diagnose debug urlfilter src-addr

Enable debug messages for selected source IP address.

```
diagnose debug urlfilter src-addr <IP address>
```

Parameter	Description	Type	Size
<IP address>	dot delimited IP address or "stop"	string	

diagnose debug urlfilter test-url

Find the result returned from the URL filter cache for a URL.

```
diagnose debug urlfilter test-url <url>
```

Parameter	Description	Type	Size
<url>	URL to test.	string	

diagnose debug urlfilter valgrind

Valgrind analysis.

```
diagnose debug urlfilter valgrind
```

diagnose debug urlfilter valgrind disable

Force daemon to restart.

```
diagnose debug urlfilter valgrind disable
```

diagnose debug urlfilter valgrind enable

Force daemon to restart.

```
diagnose debug urlfilter valgrind enable
```

diagnose debug urlfilter valgrind log

Valgrind logs.

```
diagnose debug urlfilter valgrind log
```

diagnose debug urlfilter valgrind log clear

Clear logs.

```
diagnose debug urlfilter valgrind log clear
```

diagnose debug urlfilter valgrind log show

Show logs.

```
diagnose debug urlfilter valgrind log show
```

diagnose debug urlfilter valgrind memcheck

Force daemon to restart.

```
diagnose debug urlfilter valgrind memcheck
```

diagnose debug urlfilter valgrind memcheck_less

Force daemon to restart.

```
diagnose debug urlfilter valgrind memcheck_less
```


diagnose debug urlfilter valgrind status

Show valgrind status.

```
diagnose debug urlfilter valgrind status
```

diagnose debug user

Local/admin user name

```
diagnose debug user
```

diagnose debug user hash

Display hashed user name.

```
diagnose debug user hash <String>
```

Parameter	Description	Type	Size
<String>	user name	string	

diagnose debug user list

List local/admin user name.

```
diagnose debug user list
```

diagnose debug vm-print-license

Print license info

```
diagnose debug vm-print-license
```

diagnose debug vpce

Print kernel vpce info.

```
diagnose debug vpce
```

diagnose disktest

Disk test

This topic includes the following commands:

- [diagnose disktest block on page 2802](#)
- [diagnose disktest block 1 on page 2802](#)
- [diagnose disktest block 16 on page 2802](#)
- [diagnose disktest block 256 on page 2802](#)
- [diagnose disktest block 4 on page 2803](#)
- [diagnose disktest block 64 on page 2803](#)
- [diagnose disktest device on page 2803](#)
- [diagnose disktest run on page 2803](#)
- [diagnose disktest size on page 2803](#)
- [diagnose disktest time on page 2804](#)

diagnose disktest block

Block size of each read/write operation.

```
diagnose disktest block
```

diagnose disktest block 1

1M

```
diagnose disktest block 1
```

diagnose disktest block 16

16M

```
diagnose disktest block 16
```

diagnose disktest block 256

256M

```
diagnose disktest block 256
```

diagnose disktest block 4

4M

```
diagnose disktest block 4
```

diagnose disktest block 64

64M

```
diagnose disktest block 64
```

diagnose disktest device

Device to test.

```
diagnose disktest device
```

diagnose disktest run

Run test with specified cycles (default = no limit).

```
diagnose disktest run <Integer>
```

Parameter	Description	Type	Size
<Integer>	Enter test cycles (default = no limit).	string	

diagnose disktest size

Test size limit for each cycle (default = no limit).

```
diagnose disktest size <Integer>
```

Parameter	Description	Type	Size
<Integer>	Enter test size limit for each cycle in MB (default = no limit).	string	

diagnose disktest time

Test time limit for each cycle (default = no limit).

```
diagnose disktest time <Integer>
```

Parameter	Description	Type	Size
<Integer>	Enter test time limit for each cycle in seconds (default = no limit).	string	

diagnose dpdk config

DPDK config.

This topic includes the following commands:

- [diagnose dpdk config show on page 2804](#)

diagnose dpdk config show

Show DPDK configs.

```
diagnose dpdk config show
```

diagnose dpdk log clear

Clear DPDK system logs - please select which log to clear.

This topic includes the following commands:

- [diagnose dpdk log clear early-init on page 2804](#)

diagnose dpdk log clear early-init

Clear DPDK early init logs.

```
diagnose dpdk log clear early-init
```

diagnose dpdk log show

Show DPDK system logs - please select which log to show.

This topic includes the following commands:

- [diagnose dpdk log show early-init on page 2805](#)

diagnose dpdk log show early-init

DPDK early init logs.

```
diagnose dpdk log show early-init
```

diagnose dpdk performance

DPDK performance status, e.g. CPU usage.

This topic includes the following commands:

- [diagnose dpdk performance show on page 2805](#)

diagnose dpdk performance show

Show DPDK performance status.

```
diagnose dpdk performance show
```

diagnose dpdk statistics clear

Clear all DPDK statistics.

This topic includes the following commands:

- [diagnose dpdk statistics clear all on page 2805](#)

diagnose dpdk statistics clear all

Clear all DPDK statistics.

```
diagnose dpdk statistics clear all
```

diagnose dpdk statistics show

Show DPDK statistics - please select which stats to show.

This topic includes the following commands:

- [diagnose dpdk statistics show engine on page 2806](#)
- [diagnose dpdk statistics show ipsec on page 2806](#)
- [diagnose dpdk statistics show memory on page 2806](#)
- [diagnose dpdk statistics show port on page 2806](#)
- [diagnose dpdk statistics show vnp on page 2807](#)

diagnose dpdk statistics show engine

Show per-engine DPDK statistics.

```
diagnose dpdk statistics show engine
```

diagnose dpdk statistics show ipsec

Show IPSec SA table and SPI session table statistics.

```
diagnose dpdk statistics show ipsec
```

diagnose dpdk statistics show memory

Show DPDK hugepage memory statistics.

```
diagnose dpdk statistics show memory
```

diagnose dpdk statistics show port

Show per-port DPDK statistics.

```
diagnose dpdk statistics show port
```

diagnose dpdk statistics show vnp

Show per-VNP engine DPDK statistics.

```
diagnose dpdk statistics show vnp
```

diagnose dpdk version

DPDK version.

This topic includes the following commands:

- [diagnose dpdk version show on page 2807](#)

diagnose dpdk version show

Show DPDK version.

```
diagnose dpdk version show
```

diagnose emailfilter

emailfilter

This topic includes the following commands:

- [diagnose emailfilter bword on page 2807](#)
- [diagnose emailfilter bword matchfilter on page 2808](#)
- [diagnose emailfilter fortishield on page 2808](#)
- [diagnose emailfilter fortishield servers on page 2808](#)
- [diagnose emailfilter fortishield statistics on page 2808](#)
- [diagnose emailfilter fortishield statistics flush on page 2808](#)
- [diagnose emailfilter fortishield statistics list on page 2809](#)

diagnose emailfilter bword

Spam banned word match filter.

```
diagnose emailfilter bword
```

diagnose emailfilter bword matchfilter

Filtered list display.

```
diagnose emailfilter bword matchfilter <filter string>
```

Parameter	Description	Type	Size
<filter string>	Filter string from end of spam filter banned word log line. For example: '1-n8 4 0 1 4 10 nC 4'	string	

diagnose emailfilter fortishield

FortiGuard

```
diagnose emailfilter fortishield
```

diagnose emailfilter fortishield servers

FortiGuard-AntiSpam server status.

```
diagnose emailfilter fortishield servers <refresh-rate>
```

Parameter	Description	Type	Size
<refresh-rate>	Frequency to refresh server list (sec).	string	

diagnose emailfilter fortishield statistics

FortiGuard-AntiSpam cache and daemon statistics.

```
diagnose emailfilter fortishield statistics
```

diagnose emailfilter fortishield statistics flush

Flush cache and daemon statistics.

```
diagnose emailfilter fortishield statistics flush
```


diagnose emailfilter fortishield statistics list

Display server status, cache and daemon statistics.

```
diagnose emailfilter fortishield statistics list
```

diagnose endpoint

Endpoint compliance diagnostics.

This topic includes the following commands:

- [diagnose endpoint avatar on page 2811](#)
- [diagnose endpoint avatar allow-nodisk on page 2811](#)
- [diagnose endpoint avatar cleanup on page 2811](#)
- [diagnose endpoint avatar find on page 2811](#)
- [diagnose endpoint avatar find fingerprint on page 2812](#)
- [diagnose endpoint avatar find uid on page 2812](#)
- [diagnose endpoint avatar list on page 2812](#)
- [diagnose endpoint avatar list active on page 2812](#)
- [diagnose endpoint avatar list all on page 2812](#)
- [diagnose endpoint avatar list inactive on page 2813](#)
- [diagnose endpoint avatar purge-all on page 2813](#)
- [diagnose endpoint debug-zone on page 2813](#)
- [diagnose endpoint debug-zone background-debug on page 2813](#)
- [diagnose endpoint debug-zone dump on page 2813](#)
- [diagnose endpoint debug-zone set-lls-quota on page 2814](#)
- [diagnose endpoint ec-shm on page 2814](#)
- [diagnose endpoint ec-shm delete on page 2814](#)
- [diagnose endpoint ec-shm find-by-ipvd on page 2814](#)
- [diagnose endpoint ec-shm find-by-uid on page 2815](#)
- [diagnose endpoint ec-shm list on page 2815](#)
- [diagnose endpoint ec-shm summary on page 2815](#)
- [diagnose endpoint ec-shm update-by-json on page 2815](#)
- [diagnose endpoint fctems on page 2816](#)
- [diagnose endpoint fctems api-status on page 2816](#)
- [diagnose endpoint fctems api-status clear on page 2816](#)
- [diagnose endpoint fctems cloud-server on page 2816](#)
- [diagnose endpoint fctems custom on page 2817](#)
- [diagnose endpoint fctems ec-shm-dump on page 2817](#)
- [diagnose endpoint fctems get-pub-addr on page 2817](#)
- [diagnose endpoint fctems info on page 2817](#)

- [diagnose endpoint fctems info pause on page 2818](#)
- [diagnose endpoint fctems info pre-master-key on page 2818](#)
- [diagnose endpoint fctems info protocol on page 2818](#)
- [diagnose endpoint fctems info repeat on page 2818](#)
- [diagnose endpoint fctems info repeat data-in on page 2818](#)
- [diagnose endpoint fctems info repeat data-out on page 2819](#)
- [diagnose endpoint fctems info repeat header-in on page 2819](#)
- [diagnose endpoint fctems info repeat header-out on page 2819](#)
- [diagnose endpoint fctems info repeat ssl-data-in on page 2819](#)
- [diagnose endpoint fctems info repeat ssl-data-out on page 2819](#)
- [diagnose endpoint fctems info repeat textinfo on page 2820](#)
- [diagnose endpoint fctems info reset on page 2820](#)
- [diagnose endpoint fctems info resume on page 2820](#)
- [diagnose endpoint fctems json on page 2820](#)
- [diagnose endpoint fctems json deep-inspect-cert-sync on page 2820](#)
- [diagnose endpoint fctems json gateway-mac-request on page 2821](#)
- [diagnose endpoint fctems queue-complete-calls on page 2821](#)
- [diagnose endpoint fctems test-authorization on page 2821](#)
- [diagnose endpoint fctems test-connectivity on page 2821](#)
- [diagnose endpoint fctems wss-cert-skip-check on page 2821](#)
- [diagnose endpoint filter on page 2822](#)
- [diagnose endpoint filter avatar-fingerprint on page 2822](#)
- [diagnose endpoint filter clear on page 2822](#)
- [diagnose endpoint filter ems-sn on page 2822](#)
- [diagnose endpoint filter ftcl-uid on page 2822](#)
- [diagnose endpoint filter list on page 2823](#)
- [diagnose endpoint filter record-debug-log on page 2823](#)
- [diagnose endpoint filter show-large-data on page 2823](#)
- [diagnose endpoint lls-comm on page 2823](#)
- [diagnose endpoint lls-comm connect on page 2823](#)
- [diagnose endpoint lls-comm disconnect on page 2824](#)
- [diagnose endpoint lls-comm recv on page 2824](#)
- [diagnose endpoint lls-comm send on page 2824](#)
- [diagnose endpoint lls-comm send echo on page 2824](#)
- [diagnose endpoint lls-comm send echo echo on page 2824](#)
- [diagnose endpoint lls-comm send general on page 2825](#)
- [diagnose endpoint lls-comm send general get-index on page 2825](#)
- [diagnose endpoint lls-comm send general register on page 2825](#)
- [diagnose endpoint lls-comm send general unregister on page 2825](#)
- [diagnose endpoint lls-comm send ping on page 2825](#)
- [diagnose endpoint lls-comm send ping set-interval on page 2826](#)
- [diagnose endpoint lls-comm send ztna on page 2826](#)
- [diagnose endpoint lls-comm send ztna find-ip-vdom on page 2826](#)

- [diagnose endpoint lls-comm send ztna find-uid on page 2826](#)
- [diagnose endpoint lls-comm send ztna message-format on page 2827](#)
- [diagnose endpoint lls-comm send ztna subscribe-all on page 2827](#)
- [diagnose endpoint lls-comm send ztna unsubscribe-all on page 2827](#)
- [diagnose endpoint lls-comm send ztna unsubscribe-uid on page 2827](#)
- [diagnose endpoint lls-comm status on page 2828](#)
- [diagnose endpoint tags on page 2828](#)
- [diagnose endpoint tags remove-by-id on page 2828](#)
- [diagnose endpoint tags remove-by-name on page 2828](#)
- [diagnose endpoint tags remove-by-name-legacy on page 2828](#)
- [diagnose endpoint tags remove-by-sn on page 2829](#)
- [diagnose endpoint tags test-common-tag-update on page 2829](#)

diagnose endpoint avatar

FortiClient avatar.

```
diagnose endpoint avatar
```

diagnose endpoint avatar allow-nodisk

Allow no disk for avatar

```
diagnose endpoint avatar allow-nodisk [enable|disable]
```

Parameter	Description	Type	Size
[enable disable]	Allow saving avatars on non-harddisk storage.	string	

diagnose endpoint avatar cleanup

Purge all inactive avatars

```
diagnose endpoint avatar cleanup
```

diagnose endpoint avatar find

Find avatar location

```
diagnose endpoint avatar find
```

diagnose endpoint avatar find fingerprint

Find avatar by fingerprint

```
diagnose endpoint avatar find fingerprint <fingerprint>
```

Parameter	Description	Type	Size
<fingerprint>	Avatar fingerprint	string	

diagnose endpoint avatar find uid

Find avatar by uid/user/domain

```
diagnose endpoint avatar find uid <ftcl-uid> <user-name> <domain>
```

Parameter	Description	Type	Size
<ftcl-uid>	FortiClient UID	string	
<user-name>	User name	string	
<domain>	User domain	string	

diagnose endpoint avatar list

Display avatars

```
diagnose endpoint avatar list
```

diagnose endpoint avatar list active

Display active avatars

```
diagnose endpoint avatar list active <number>
```

Parameter	Description	Type	Size
<number>	Number of files to display per page.	string	

diagnose endpoint avatar list all

Display all avatars

```
diagnose endpoint avatar list all <number>
```

Parameter	Description	Type	Size
<number>	Number of files to display per page.	string	

diagnose endpoint avatar list inactive

Display inactive avatars

```
diagnose endpoint avatar list inactive <number>
```

Parameter	Description	Type	Size
<number>	Number of files to display per page.	string	

diagnose endpoint avatar purge-all

Purge ALL avatars

```
diagnose endpoint avatar purge-all
```

diagnose endpoint debug-zone

Debug Zone.

```
diagnose endpoint debug-zone
```

diagnose endpoint debug-zone background-debug

Background Debugs.

```
diagnose endpoint debug-zone background-debug <val>
```

Parameter	Description	Type	Size
<val>	Value (enable disable)	string	

diagnose endpoint debug-zone dump

Dump all debug zone info.

```
diagnose endpoint debug-zone dump
```

diagnose endpoint debug-zone set-lls-quota

Set send quota for each socket

```
diagnose endpoint debug-zone set-lls-quota <quota>
```

Parameter	Description	Type	Size
<quota>	Quota in bytes	string	

diagnose endpoint ec-shm

Endpoint record.

```
diagnose endpoint ec-shm
```

diagnose endpoint ec-shm delete

Delete endpoint records.

```
diagnose endpoint ec-shm delete <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Source IPv4 address.	string	

diagnose endpoint ec-shm find-by-ipvd

Display record by IP and vdom.

```
diagnose endpoint ec-shm find-by-ipvd <ipv4-address> <vdom-name>
```

Parameter	Description	Type	Size
<ipv4-address>	Endpoint IPv4 address.	string	
<vdom-name>	VDOM name of the client.	string	

diagnose endpoint ec-shm find-by-uid

Display record by Client UID.

```
diagnose endpoint ec-shm find-by-uid <ftct-uid> <emssn> <ems-tenant-id>
```

Parameter	Description	Type	Size
<ftct-uid>	Client UID	string	
<emssn>	EMS Serial Number	string	
<ems-tenant-id>	EMS Tenant ID	string	

diagnose endpoint ec-shm list

Display all records for one EMS.

```
diagnose endpoint ec-shm list <ipv4-address> <mac-address> <emssn> <ems-tenant-id>
```

Parameter	Description	Type	Size
<ipv4-address>	Source IPv4 address ("" for all IP addresses).	string	
<mac-address>	Source MAC address ("" for all MAC addresses).	string	
<emssn>	EMS Serial Number	string	
<ems-tenant-id>	EMS Tenant ID	string	

diagnose endpoint ec-shm summary

List summary of endpoint records.

```
diagnose endpoint ec-shm summary
```

diagnose endpoint ec-shm update-by-json

Add endpoint record by JSON.

```
diagnose endpoint ec-shm update-by-json <uid> <ems-sn> <ems-tenant-id> <json>
```

Parameter	Description	Type	Size
<uid>	FortiClient UID.	string	
<ems-sn>	FortiClient EMS serial number.	string	
<ems-tenant-id>	FortiClient EMS tenant ID.	string	
<json>	JSON string.	string	

diagnose endpoint fctems

FortiClient EMS.

```
diagnose endpoint fctems
```

diagnose endpoint fctems api-status

Tools to diagnose EMS API status.

```
diagnose endpoint fctems api-status
```

diagnose endpoint fctems api-status clear

Clear EMS API status.

```
diagnose endpoint fctems api-status clear <fctems>
```

Parameter	Description	Type	Size
<fctems>	FortiClient EMS table entry name in CMDB.	string	

diagnose endpoint fctems cloud-server

cloud server type.

```
diagnose endpoint fctems cloud-server <type>
```

Parameter	Description	Type	Size
<type>	FortiClient EMS cloud server type(0, 1 or 2), 0-Production, 1-Development and 2-Beta.	string	

diagnose endpoint fctems custom

Custom API.

```
diagnose endpoint fctems custom <ems-id> <entry-point> <method> <data-param-type> <data>
```

Parameter	Description	Type	Size
<ems-id>	ems id.	string	
<entry-point>	entry point.	string	
<method>	HTTP method.	string	
<data-param-type>	data parameter type.	string	
<data>	data	string	

diagnose endpoint fctems ec-shm-dump

Dump endpoint record shm.

```
diagnose endpoint fctems ec-shm-dump <fctems>
```

Parameter	Description	Type	Size
<fctems>	FortiClient EMS table entry id in CMDB.	string	

diagnose endpoint fctems get-pub-addr

Get FortiClient EMS public address.

```
diagnose endpoint fctems get-pub-addr <fctems>
```

Parameter	Description	Type	Size
<fctems>	FortiClient EMS table entry id in CMDB.	string	

diagnose endpoint fctems info

Get info from FortiClient EMS calls.

```
diagnose endpoint fctems info
```

diagnose endpoint fctems info pause

Pause getting info.

```
diagnose endpoint fctems info pause
```

diagnose endpoint fctems info pre-master-key

Pre-master Key.

```
diagnose endpoint fctems info pre-master-key [enable|disable]
```

Parameter	Description	Type	Size
[enable disable]	enable/disable	string	

diagnose endpoint fctems info protocol

Protocol.

```
diagnose endpoint fctems info protocol [none|https|wss|all]
```

Parameter	Description	Type	Size
[none https wss all]	none/https/wss/all	string	

diagnose endpoint fctems info repeat

Get/Set repetitions for each infotype.

```
diagnose endpoint fctems info repeat
```

diagnose endpoint fctems info repeat data-in

data in.

```
diagnose endpoint fctems info repeat data-in <num>
```

Parameter	Description	Type	Size
<num>	Integer in the range of [0, 255].	string	

diagnose endpoint fctems info repeat data-out

data out.

```
diagnose endpoint fctems info repeat data-out <num>
```

Parameter	Description	Type	Size
<num>	Integer in the range of [0, 255].	string	

diagnose endpoint fctems info repeat header-in

header in.

```
diagnose endpoint fctems info repeat header-in <num>
```

Parameter	Description	Type	Size
<num>	Integer in the range of [0, 255].	string	

diagnose endpoint fctems info repeat header-out

header out.

```
diagnose endpoint fctems info repeat header-out <num>
```

Parameter	Description	Type	Size
<num>	Integer in the range of [0, 255].	string	

diagnose endpoint fctems info repeat ssl-data-in

SSL data in.

```
diagnose endpoint fctems info repeat ssl-data-in <num>
```

Parameter	Description	Type	Size
<num>	Integer in the range of [0, 255].	string	

diagnose endpoint fctems info repeat ssl-data-out

SSL data out.

```
diagnose endpoint fctems info repeat ssl-data-out <num>
```

Parameter	Description	Type	Size
<num>	Integer in the range of [0, 255].	string	

diagnose endpoint fctems info repeat textinfo

text info.

```
diagnose endpoint fctems info repeat textinfo <num>
```

Parameter	Description	Type	Size
<num>	Integer in the range of [0, 255].	string	

diagnose endpoint fctems info reset

Reset fctems info.

```
diagnose endpoint fctems info reset
```

diagnose endpoint fctems info resume

Resume/Start getting info.

```
diagnose endpoint fctems info resume
```

diagnose endpoint fctems json

FortiClient EMS REST-API JSON test.

```
diagnose endpoint fctems json
```

diagnose endpoint fctems json deep-inspect-cert-sync

Print deep inspection certificate sync json.

```
diagnose endpoint fctems json deep-inspect-cert-sync
```

diagnose endpoint fctems json gateway-mac-request

Print gateway-info json.

```
diagnose endpoint fctems json gateway-mac-request
```

diagnose endpoint fctems queue-complete-calls

Add complete (un)quarantine call(s) to FCEMSD queue.

```
diagnose endpoint fctems queue-complete-calls <call>[,<call>[,...]]
```

Parameter	Description	Type	Size
<call>[,<call>[,...]]	Comma separated list of calls. Run without the argument for more help.	string	

diagnose endpoint fctems test-authorization

Authorization test for FortiClient EMS.

```
diagnose endpoint fctems test-authorization <fctems>
```

Parameter	Description	Type	Size
<fctems>	FortiClient EMS table entry id in CMDB.	string	

diagnose endpoint fctems test-connectivity

Connectivity test for FortiClient EMS.

```
diagnose endpoint fctems test-connectivity <fctems>
```

Parameter	Description	Type	Size
<fctems>	FortiClient EMS table entry id in CMDB.	string	

diagnose endpoint fctems wss-cert-skip-check

Skip WebSocketSecure server certificate check.

```
diagnose endpoint fctems wss-cert-skip-check [yes|no]
```

Parameter	Description	Type	Size
[yes no]	yes/no	string	

diagnose endpoint filter

Debug filter for fcnacd.

```
diagnose endpoint filter
```

diagnose endpoint filter avatar-fingerprint

Avatar fingerprint to filter by.

```
diagnose endpoint filter avatar-fingerprint <avatar-fingerprint>
```

Parameter	Description	Type	Size
<avatar-fingerprint>	Avatar fingerprint.	string	

diagnose endpoint filter clear

Erase the current filter.

```
diagnose endpoint filter clear
```

diagnose endpoint filter ems-sn

FortiClient EMS serial-number to filter by.

```
diagnose endpoint filter ems-sn <ems-sn>
```

Parameter	Description	Type	Size
<ems-sn>	EMS serial-number.	string	

diagnose endpoint filter ftcl-uid

FortiClient UID to filter by.

```
diagnose endpoint filter ftcl-uid <ftcl-uid>
```

Parameter	Description	Type	Size
<ftcl-uid>	FortiClient UID.	string	

diagnose endpoint filter list

Display the current filter.

```
diagnose endpoint filter list
```

diagnose endpoint filter record-debug-log

Record debug log.

```
diagnose endpoint filter record-debug-log [enable/disable]
```

Parameter	Description	Type	Size
[enable/disable]	Enable or disable.	string	

diagnose endpoint filter show-large-data

Show large data.

```
diagnose endpoint filter show-large-data [yes/no]
```

Parameter	Description	Type	Size
[yes/no]	Yes or no.	string	

diagnose endpoint lls-comm

Long-Lived Socket Communication.

```
diagnose endpoint lls-comm
```

diagnose endpoint lls-comm connect

Connect.

```
diagnose endpoint lls-comm connect
```

diagnose endpoint lls-comm disconnect

Disconnect.

```
diagnose endpoint lls-comm disconnect
```

diagnose endpoint lls-comm recv

Receive Messages.

```
diagnose endpoint lls-comm recv <repeat>
```

Parameter	Description	Type	Size
<repeat>	Repeat number of receives	string	

diagnose endpoint lls-comm send

Send Message.

```
diagnose endpoint lls-comm send
```

diagnose endpoint lls-comm send echo

Echo long-lived socket channel

```
diagnose endpoint lls-comm send echo
```

diagnose endpoint lls-comm send echo echo

Echo

```
diagnose endpoint lls-comm send echo echo <msg>
```

Parameter	Description	Type	Size
<msg>	Message to echo	string	

diagnose endpoint lls-comm send general

General long-lived socket channel

```
diagnose endpoint lls-comm send general
```

diagnose endpoint lls-comm send general get-index

Get Long-lived socket channel index.

```
diagnose endpoint lls-comm send general get-index
```

diagnose endpoint lls-comm send general register

Register to Long-lived Socket channel(s)

```
diagnose endpoint lls-comm send general register <channel-mask>
```

Parameter	Description	Type	Size
<channel-mask>	Channel Mask in decimal, octal or hexadecimal	string	

diagnose endpoint lls-comm send general unregister

Unregister from Long-lived Socket channel(s)

```
diagnose endpoint lls-comm send general unregister <channel-mask>
```

Parameter	Description	Type	Size
<channel-mask>	Channel Mask in decimal, octal or hexadecimal	string	

diagnose endpoint lls-comm send ping

Ping long-lived socket channel

```
diagnose endpoint lls-comm send ping
```

diagnose endpoint lls-comm send ping set-interval

Set interval

```
diagnose endpoint lls-comm send ping set-interval <interval>
```

Parameter	Description	Type	Size
<interval>	Period in units of 1/100 seconds	string	

diagnose endpoint lls-comm send ztna

ZTNA long-lived socket channel

```
diagnose endpoint lls-comm send ztna
```

diagnose endpoint lls-comm send ztna find-ip-vdom

Find by IP and VDOM

```
diagnose endpoint lls-comm send ztna find-ip-vdom <ip> <vdom>
```

Parameter	Description	Type	Size
<ip>	IPv4 or IPv6 address of client	string	
<vdom>	VDOM name	string	

diagnose endpoint lls-comm send ztna find-uid

Find by FortiClient UID and EMS SN

```
diagnose endpoint lls-comm send ztna find-uid <ftct-uid> <emssn> <ems-tenant-id>
```

Parameter	Description	Type	Size
<ftct-uid>	Client UID	string	
<emssn>	EMS Serial Number	string	
<ems-tenant-id>	EMS Tenant ID	string	

diagnose endpoint lls-comm send ztna message-format

Select if wad header is sent

```
diagnose endpoint lls-comm send ztna message-format <index>
```

Parameter	Description	Type	Size
<index>	0: standard 1: wad informer 2: diag wad informer	string	

diagnose endpoint lls-comm send ztna subscribe-all

Subscribe to all FortiClients on selected LLS bits

```
diagnose endpoint lls-comm send ztna subscribe-all <mask>
```

Parameter	Description	Type	Size
<mask>	Bit mask	string	

diagnose endpoint lls-comm send ztna unsubscribe-all

Unsubscribe to all FortiClients on issuing LLS

```
diagnose endpoint lls-comm send ztna unsubscribe-all
```

diagnose endpoint lls-comm send ztna unsubscribe-uid

Unsubscribe from FortiClient UID

```
diagnose endpoint lls-comm send ztna unsubscribe-uid <ftct-uid> <emssn> <ems-tenant-id>
```

Parameter	Description	Type	Size
<ftct-uid>	Client UID	string	
<emssn>	EMS Serial Number	string	
<ems-tenant-id>	EMS_Tenant ID	string	

diagnose endpoint lls-comm status

Status.

```
diagnose endpoint lls-comm status
```

diagnose endpoint tags

Tags.

```
diagnose endpoint tags
```

diagnose endpoint tags remove-by-id

Remove Dynamic address tags by EMS ID.

```
diagnose endpoint tags remove-by-id <EMS-ID>
```

Parameter	Description	Type	Size
<EMS-ID>	EMS ID.	string	

diagnose endpoint tags remove-by-name

Remove specific tag by EMS ID and name.

```
diagnose endpoint tags remove-by-name <TAG-Name> <EMS-ID>
```

Parameter	Description	Type	Size
<TAG-Name>	Tag name.	string	
<EMS-ID>	EMS ID.	string	

diagnose endpoint tags remove-by-name-legacy

Remove specific tag by Serial Number and name (LEGACY).

```
diagnose endpoint tags remove-by-name-legacy <TAG-Name> <SN>
```

Parameter	Description	Type	Size
<TAG-Name>	Tag name.	string	
<SN>	Serial Number.	string	

diagnose endpoint tags remove-by-sn

Remove Dynamic address tags by Serial Number (LEGACY).

```
diagnose endpoint tags remove-by-sn <SN>
```

Parameter	Description	Type	Size
<SN>	Serial Number.	string	

diagnose endpoint tags test-common-tag-update

Test update tags for FortiClient EMS

```
diagnose endpoint tags test-common-tag-update <TAG-INFO-JSON>
```

Parameter	Description	Type	Size
<TAG-INFO-JSON>	JSON string for commands.	string	

diagnose extender

Diagnostics command of extender

This topic includes the following commands:

- [diagnose extender atcmd on page 2829](#)
- [diagnose extender cmd on page 2830](#)
- [diagnose extender modem-list on page 2830](#)

diagnose extender atcmd

AT Command.

```
diagnose extender atcmd <at-command> <mark> <sn> [1|2]
```

Parameter	Description	Type	Size
<at-command>	AT command.	string	
<mark>	Change mark to '?' in AT command.	string	
<sn>	Serial number of FortiExtender.	string	
[1 2]	modem ID.	string	

diagnose extender cmd

Generic AT command.

```
diagnose extender cmd <Integer> <sn> [1|2]
```

Parameter	Description	Type	Size
<Integer>	A number mapping a generic AT command.	string	
<sn>	Serial number of FortiExtender.	string	
[1 2]	modem ID.	string	

diagnose extender modem-list

List of supported modems for FortiExtender.

```
diagnose extender modem-list
```

diagnose fdsm

FortiCloud/FortiManager Service.

This topic includes the following commands:

- [diagnose fdsm account-info on page 2831](#)
- [diagnose fdsm central-mgmt-status on page 2831](#)
- [diagnose fdsm cfg-diff on page 2831](#)
- [diagnose fdsm cfg-download on page 2832](#)
- [diagnose fdsm cfg-list on page 2832](#)
- [diagnose fdsm cfg-upload on page 2832](#)
- [diagnose fdsm contract-controller-update on page 2832](#)
- [diagnose fdsm fap-fsw-fext-contract-download on page 2833](#)

- [diagnose fdsm fc-installer-download on page 2833](#)
- [diagnose fdsm fds-update on page 2833](#)
- [diagnose fdsm fmg-auto-discovery-status on page 2833](#)
- [diagnose fdsm fortiap-download on page 2833](#)
- [diagnose fdsm fortiap-latest-ver on page 2834](#)
- [diagnose fdsm forticlient-net-info on page 2834](#)
- [diagnose fdsm forticlient-update on page 2834](#)
- [diagnose fdsm fortiex-download on page 2834](#)
- [diagnose fdsm fortiex-latest-ver on page 2834](#)
- [diagnose fdsm fortisw-download on page 2835](#)
- [diagnose fdsm fortisw-latest-ver on page 2835](#)
- [diagnose fdsm ftk-activate on page 2835](#)
- [diagnose fdsm image-download on page 2835](#)
- [diagnose fdsm image-list on page 2836](#)
- [diagnose fdsm image-upgrade-matrix on page 2836](#)
- [diagnose fdsm log-controller-update on page 2836](#)
- [diagnose fdsm message-update on page 2836](#)
- [diagnose fdsm modem-list on page 2836](#)
- [diagnose fdsm report-download on page 2836](#)
- [diagnose fdsm report-list on page 2837](#)
- [diagnose fdsm sslvpn-man-upgrade-package-download on page 2837](#)
- [diagnose fdsm sslvpn-package-download on page 2837](#)

diagnose fdsm account-info

FortiCloud account information.

```
diagnose fdsm account-info
```

diagnose fdsm central-mgmt-status

Central management registration status.

```
diagnose fdsm central-mgmt-status
```

diagnose fdsm cfg-diff

Configuration difference.

```
diagnose fdsm cfg-diff <revision1> <revision2>
```

Parameter	Description	Type	Size
<revision1>	Revision	string	
<revision2>	Revision	string	

diagnose fdsm cfg-download

Download configuration.

```
diagnose fdsm cfg-download <type> <revision>
```

Parameter	Description	Type	Size
<type>	Configuration type (normal, template, script).	string	
<revision>	Revision	string	

diagnose fdsm cfg-list

Download configuration list.

```
diagnose fdsm cfg-list <type>
```

Parameter	Description	Type	Size
<type>	Configuration type (normal, template, script).	string	

diagnose fdsm cfg-upload

Upload configuration.

```
diagnose fdsm cfg-upload <comments>
```

Parameter	Description	Type	Size
<comments>	Comments	string	

diagnose fdsm contract-controller-update

Update contract controller.

```
diagnose fdsm contract-controller-update
```


diagnose fdsm fap-fsw-fext-contract-download

FAP/FSW/FEX contract information.

```
diagnose fdsm fap-fsw-fext-contract-download <serial1*serial2*...> <cache>
```

Parameter	Description	Type	Size
<serial1*serial2*...>	Serial numbers of FAP/FSW/FEX devices	string	
<cache>	[yes/no]	string	

diagnose fdsm fc-installer-download

Download FortiClient installer.

```
diagnose fdsm fc-installer-download <id>
```

Parameter	Description	Type	Size
<id>	Installer ID.	string	

diagnose fdsm fds-update

Perform FortiGuard update.

```
diagnose fdsm fds-update
```

diagnose fdsm fmg-auto-discovery-status

FortiManager auto-discovery status.

```
diagnose fdsm fmg-auto-discovery-status
```

diagnose fdsm fortiap-download

Download FortiAP image.

```
diagnose fdsm fortiap-download <id>
```

Parameter	Description	Type	Size
<id>	Image ID	string	

diagnose fdsm fortiap-latest-ver

Get most recent FortiAP build information.

```
diagnose fdsm fortiap-latest-ver <model> <version>
```

Parameter	Description	Type	Size
<model>	Model name or "" to get all models	string	
<version>	FortiOS version, in the format of major.minor.patch, e.g. 6.4.2	string	

diagnose fdsm forticlient-net-info

FortiClient net information.

```
diagnose fdsm forticlient-net-info
```

diagnose fdsm forticlient-update

FortiClient update.

```
diagnose fdsm forticlient-update
```

diagnose fdsm fortiox-download

Download FortiExtender image.

```
diagnose fdsm fortiox-download <id>
```

Parameter	Description	Type	Size
<id>	Image ID	string	

diagnose fdsm fortiox-latest-ver

Get most recent FortiExtender build information.

```
diagnose fdsm fortiox-latest-ver <model> <version>
```

Parameter	Description	Type	Size
<model>	Model name or "" to get all models	string	
<version>	FortiOS version, in the format of major.minor.patch, e.g. 6.4.2	string	

diagnose fdsm fortisw-download

Download FortiSwitch image.

```
diagnose fdsm fortisw-download <id>
```

Parameter	Description	Type	Size
<id>	Image ID	string	

diagnose fdsm fortisw-latest-ver

Get most recent FortiSwitch build information.

```
diagnose fdsm fortisw-latest-ver <model> <version>
```

Parameter	Description	Type	Size
<model>	Model name or "" to get all models	string	
<version>	FortiOS version, in the format of major.minor.patch, e.g. 6.4.2	string	

diagnose fdsm ftk-activate

FortiToken activation.

```
diagnose fdsm ftk-activate
```

diagnose fdsm image-download

Download image.

```
diagnose fdsm image-download <id>
```

Parameter	Description	Type	Size
<id>	Image ID.	string	

diagnose fdsm image-list

Download image list.

```
diagnose fdsm image-list
```

diagnose fdsm image-upgrade-matrix

Download image upgrade matrix.

```
diagnose fdsm image-upgrade-matrix
```

diagnose fdsm log-controller-update

Perform log update.

```
diagnose fdsm log-controller-update
```

diagnose fdsm message-update

Perform message update.

```
diagnose fdsm message-update
```

diagnose fdsm modem-list

MODEM list.

```
diagnose fdsm modem-list
```

diagnose fdsm report-download

Download report.

```
diagnose fdsm report-download <oid>
```

Parameter	Description	Type	Size
<oid>	OID	string	

diagnose fdsm report-list

Download report list.

```
diagnose fdsm report-list <vdom>
```

Parameter	Description	Type	Size
<vdom>	VDOM Name.	string	

diagnose fdsm sslvpn-man-upgrade-package-download

Download Agentless VPN manual upgrade package.

```
diagnose fdsm sslvpn-man-upgrade-package-download <id>
```

Parameter	Description	Type	Size
<id>	Package ID.	string	

diagnose fdsm sslvpn-package-download

Download Agentless VPN package.

```
diagnose fdsm sslvpn-package-download <id>
```

Parameter	Description	Type	Size
<id>	Package ID.	string	

diagnose ffdb-fqdn

Internet service FQDN database.

This topic includes the following commands:

- [diagnose ffdb-fqdn custom-get on page 2838](#)
- [diagnose ffdb-fqdn custom-list on page 2838](#)

diagnose ffdb-fqdn custom-get

Get built-in custom name based on given FQDN.

```
diagnose ffdb-fqdn custom-get <BuiltIn FQDN-name>
```

Parameter	Description	Type	Size
<BuiltIn FQDN-name>	Built-in FQDN name	string	

diagnose ffdb-fqdn custom-list

List all built-in Internet service database (FFDB) FQDNs

```
diagnose ffdb-fqdn custom-list <BuiltIn-custom-name>
```

Parameter	Description	Type	Size
<BuiltIn-custom-name>	Show custom FQDN list for the given built-in Internet service.	string	

diagnose firewall

Firewall

This topic includes the following commands:

- [diagnose firewall auth on page 2845](#)
- [diagnose firewall auth clear on page 2845](#)
- [diagnose firewall auth filter on page 2845](#)
- [diagnose firewall auth filter clear on page 2845](#)
- [diagnose firewall auth filter group on page 2845](#)
- [diagnose firewall auth filter mac on page 2845](#)
- [diagnose firewall auth filter method on page 2846](#)
- [diagnose firewall auth filter policy on page 2846](#)
- [diagnose firewall auth filter source on page 2846](#)
- [diagnose firewall auth filter source6 on page 2847](#)
- [diagnose firewall auth filter user on page 2847](#)
- [diagnose firewall auth ipv6 on page 2847](#)
- [diagnose firewall auth ipv6 clear on page 2847](#)
- [diagnose firewall auth ipv6 list on page 2848](#)

- [diagnose firewall auth list on page 2848](#)
- [diagnose firewall auth mac on page 2848](#)
- [diagnose firewall auth mac clear on page 2848](#)
- [diagnose firewall auth mac list on page 2848](#)
- [diagnose firewall blocking on page 2848](#)
- [diagnose firewall blocking list on page 2849](#)
- [diagnose firewall dns-xlate on page 2849](#)
- [diagnose firewall dns-xlate mapping on page 2849](#)
- [diagnose firewall dns-xlate mapping list on page 2849](#)
- [diagnose firewall dns-xlate pool on page 2849](#)
- [diagnose firewall dns-xlate pool list on page 2849](#)
- [diagnose firewall dynamic on page 2850](#)
- [diagnose firewall dynamic address on page 2850](#)
- [diagnose firewall dynamic list on page 2850](#)
- [diagnose firewall dynamic test-common-tag-update on page 2850](#)
- [diagnose firewall dynamic6 on page 2850](#)
- [diagnose firewall dynamic6 address on page 2851](#)
- [diagnose firewall dynamic6 list on page 2851](#)
- [diagnose firewall fqdn on page 2851](#)
- [diagnose firewall fqdn get-ip on page 2851](#)
- [diagnose firewall fqdn get-mac on page 2851](#)
- [diagnose firewall fqdn getinfo-ip on page 2852](#)
- [diagnose firewall fqdn getinfo-mac on page 2852](#)
- [diagnose firewall fqdn list-all on page 2852](#)
- [diagnose firewall fqdn list-ip on page 2852](#)
- [diagnose firewall fqdn list-mac on page 2852](#)
- [diagnose firewall fqdn6 on page 2853](#)
- [diagnose firewall fqdn6 list on page 2853](#)
- [diagnose firewall internet-service on page 2853](#)
- [diagnose firewall internet-service list on page 2853](#)
- [diagnose firewall internet-service-app-ctrl on page 2853](#)
- [diagnose firewall internet-service-app-ctrl list on page 2853](#)
- [diagnose firewall internet-service-app-ctrl6 on page 2854](#)
- [diagnose firewall internet-service-app-ctrl6 list on page 2854](#)
- [diagnose firewall internet-service-cache on page 2854](#)
- [diagnose firewall internet-service-cache list on page 2854](#)
- [diagnose firewall internet-service-custom on page 2854](#)
- [diagnose firewall internet-service-custom list on page 2855](#)
- [diagnose firewall internet-service-disable on page 2855](#)
- [diagnose firewall internet-service-disable list on page 2855](#)
- [diagnose firewall internet-service-extension on page 2855](#)
- [diagnose firewall internet-service-extension list on page 2855](#)
- [diagnose firewall internet-service-prio-id on page 2856](#)

- [diagnose firewall internet-service-prio-id list on page 2856](#)
- [diagnose firewall internet-service6 on page 2856](#)
- [diagnose firewall internet-service6 list on page 2856](#)
- [diagnose firewall internet-service6-cache on page 2856](#)
- [diagnose firewall internet-service6-cache list on page 2856](#)
- [diagnose firewall internet-service6-custom on page 2857](#)
- [diagnose firewall internet-service6-custom list on page 2857](#)
- [diagnose firewall internet-service6-disable on page 2857](#)
- [diagnose firewall internet-service6-disable list on page 2857](#)
- [diagnose firewall internet-service6-extension on page 2857](#)
- [diagnose firewall internet-service6-extension list on page 2858](#)
- [diagnose firewall internet-service6-prio-id on page 2858](#)
- [diagnose firewall internet-service6-prio-id list on page 2858](#)
- [diagnose firewall ip-translation on page 2858](#)
- [diagnose firewall ip-translation list on page 2858](#)
- [diagnose firewall ipgeo on page 2858](#)
- [diagnose firewall ipgeo copyright-notice on page 2859](#)
- [diagnose firewall ipgeo country-list on page 2859](#)
- [diagnose firewall ipgeo ip-list on page 2859](#)
- [diagnose firewall ipgeo ip2country on page 2859](#)
- [diagnose firewall ipgeo ip6-list on page 2859](#)
- [diagnose firewall ipgeo override on page 2860](#)
- [diagnose firewall iplist on page 2860](#)
- [diagnose firewall iplist list on page 2860](#)
- [diagnose firewall iplist list optimized on page 2860](#)
- [diagnose firewall iplist6 on page 2860](#)
- [diagnose firewall iplist6 list on page 2860](#)
- [diagnose firewall iplist6 list optimized on page 2861](#)
- [diagnose firewall ipmac on page 2861](#)
- [diagnose firewall ipmac add on page 2861](#)
- [diagnose firewall ipmac delete on page 2861](#)
- [diagnose firewall ipmac list on page 2861](#)
- [diagnose firewall ipmac status on page 2862](#)
- [diagnose firewall ippool on page 2862](#)
- [diagnose firewall ippool filter on page 2862](#)
- [diagnose firewall ippool filter clear on page 2862](#)
- [diagnose firewall ippool filter name on page 2862](#)
- [diagnose firewall ippool list on page 2862](#)
- [diagnose firewall ippool list nat-ip on page 2863](#)
- [diagnose firewall ippool list pba on page 2863](#)
- [diagnose firewall ippool list user on page 2863](#)
- [diagnose firewall ippool reset-log-stats on page 2863](#)
- [diagnose firewall ippool stats on page 2863](#)

- [diagnose firewall ippool-all on page 2863](#)
- [diagnose firewall ippool-all list on page 2864](#)
- [diagnose firewall ippool-all stats on page 2864](#)
- [diagnose firewall ippool-fixed-range on page 2864](#)
- [diagnose firewall ippool-fixed-range list on page 2864](#)
- [diagnose firewall ippool-fixed-range list natip on page 2864](#)
- [diagnose firewall ippool-nptv6 on page 2865](#)
- [diagnose firewall ippool-nptv6 natip on page 2865](#)
- [diagnose firewall iprope on page 2865](#)
- [diagnose firewall iprope appctrl on page 2865](#)
- [diagnose firewall iprope appctrl list on page 2865](#)
- [diagnose firewall iprope appctrl shaper on page 2865](#)
- [diagnose firewall iprope appctrl shaper list on page 2866](#)
- [diagnose firewall iprope appctrl stats on page 2866](#)
- [diagnose firewall iprope appctrl stats clear on page 2866](#)
- [diagnose firewall iprope appctrl stats list on page 2866](#)
- [diagnose firewall iprope appctrl status on page 2866](#)
- [diagnose firewall iprope clear on page 2866](#)
- [diagnose firewall iprope list on page 2867](#)
- [diagnose firewall iprope lookup on page 2867](#)
- [diagnose firewall iprope show on page 2867](#)
- [diagnose firewall iprope state on page 2868](#)
- [diagnose firewall iprope top on page 2868](#)
- [diagnose firewall iprope6 on page 2868](#)
- [diagnose firewall iprope6 clear on page 2868](#)
- [diagnose firewall iprope6 list on page 2868](#)
- [diagnose firewall iprope6 lookup on page 2869](#)
- [diagnose firewall iprope6 show on page 2869](#)
- [diagnose firewall iprope6 state on page 2869](#)
- [diagnose firewall iprope6 top on page 2870](#)
- [diagnose firewall ipv6-ehf on page 2870](#)
- [diagnose firewall ipv6-ehf list on page 2870](#)
- [diagnose firewall network-service-dynamic on page 2870](#)
- [diagnose firewall network-service-dynamic list on page 2870](#)
- [diagnose firewall ngfw-fix-application on page 2871](#)
- [diagnose firewall ngfw-fix-application list on page 2871](#)
- [diagnose firewall packet on page 2871](#)
- [diagnose firewall packet distribution on page 2871](#)
- [diagnose firewall pcp-mapping on page 2871](#)
- [diagnose firewall pcp-mapping filter on page 2871](#)
- [diagnose firewall pcp-mapping filter clear on page 2872](#)
- [diagnose firewall pcp-mapping filter client-ip on page 2872](#)
- [diagnose firewall pcp-mapping filter ext-ip on page 2872](#)

- [diagnose firewall pcp-mapping filter ext-port on page 2872](#)
- [diagnose firewall pcp-mapping filter intl-ip on page 2873](#)
- [diagnose firewall pcp-mapping filter intl-port on page 2873](#)
- [diagnose firewall pcp-mapping filter pool on page 2873](#)
- [diagnose firewall pcp-mapping filter protocol on page 2873](#)
- [diagnose firewall pcp-mapping filter remote-ip on page 2874](#)
- [diagnose firewall pcp-mapping filter remote-port on page 2874](#)
- [diagnose firewall pcp-mapping flush on page 2874](#)
- [diagnose firewall pcp-mapping flush inbound on page 2874](#)
- [diagnose firewall pcp-mapping flush outbound on page 2874](#)
- [diagnose firewall pcp-mapping list on page 2875](#)
- [diagnose firewall pcp-mapping list inbound on page 2875](#)
- [diagnose firewall pcp-mapping list outbound on page 2875](#)
- [diagnose firewall proute on page 2875](#)
- [diagnose firewall proute clear on page 2875](#)
- [diagnose firewall proute list on page 2875](#)
- [diagnose firewall proute show on page 2876](#)
- [diagnose firewall proute6 on page 2876](#)
- [diagnose firewall proute6 clear on page 2876](#)
- [diagnose firewall proute6 list on page 2876](#)
- [diagnose firewall proute6 show on page 2876](#)
- [diagnose firewall route_tag on page 2877](#)
- [diagnose firewall route_tag list on page 2877](#)
- [diagnose firewall route_tag_v6 on page 2877](#)
- [diagnose firewall route_tag_v6 list on page 2877](#)
- [diagnose firewall schedule on page 2877](#)
- [diagnose firewall schedule debug on page 2878](#)
- [diagnose firewall schedule list on page 2878](#)
- [diagnose firewall schedule reload on page 2878](#)
- [diagnose firewall sf-addresses on page 2878](#)
- [diagnose firewall sf-addresses list on page 2878](#)
- [diagnose firewall shaper on page 2878](#)
- [diagnose firewall shaper dynamic-shaper on page 2879](#)
- [diagnose firewall shaper dynamic-shaper flush on page 2879](#)
- [diagnose firewall shaper dynamic-shaper list on page 2879](#)
- [diagnose firewall shaper dynamic-shaper list ip on page 2879](#)
- [diagnose firewall shaper dynamic-shaper list ipv6 on page 2879](#)
- [diagnose firewall shaper dynamic-shaper list user on page 2880](#)
- [diagnose firewall shaper dynamic-shaper stats on page 2880](#)
- [diagnose firewall shaper per-ip-shaper on page 2880](#)
- [diagnose firewall shaper per-ip-shaper clear on page 2880](#)
- [diagnose firewall shaper per-ip-shaper list on page 2880](#)
- [diagnose firewall shaper per-ip-shaper state on page 2880](#)

- [diagnose firewall shaper per-ip-shaper stats on page 2881](#)
- [diagnose firewall shaper traffic-shaper on page 2881](#)
- [diagnose firewall shaper traffic-shaper list on page 2881](#)
- [diagnose firewall shaper traffic-shaper state on page 2881](#)
- [diagnose firewall shaper traffic-shaper stats on page 2881](#)
- [diagnose firewall shaper traffic-shaper stats clear on page 2881](#)
- [diagnose firewall shaper traffic-shaper stats list on page 2882](#)
- [diagnose firewall uuid on page 2882](#)
- [diagnose firewall uuid list on page 2882](#)
- [diagnose firewall vendor-mac on page 2882](#)
- [diagnose firewall vendor-mac list on page 2882](#)
- [diagnose firewall vip on page 2882](#)
- [diagnose firewall vip realserver on page 2883](#)
- [diagnose firewall vip realserver clear on page 2883](#)
- [diagnose firewall vip realserver clear vip on page 2883](#)
- [diagnose firewall vip realserver clear vip6 on page 2883](#)
- [diagnose firewall vip realserver down on page 2883](#)
- [diagnose firewall vip realserver healthcheck on page 2884](#)
- [diagnose firewall vip realserver healthcheck stats on page 2884](#)
- [diagnose firewall vip realserver healthcheck stats clear on page 2884](#)
- [diagnose firewall vip realserver healthcheck stats show on page 2884](#)
- [diagnose firewall vip realserver list on page 2884](#)
- [diagnose firewall vip realserver up on page 2885](#)
- [diagnose firewall vip virtual-server on page 2885](#)
- [diagnose firewall vip virtual-server filter on page 2885](#)
- [diagnose firewall vip virtual-server filter clear on page 2885](#)
- [diagnose firewall vip virtual-server filter dst on page 2885](#)
- [diagnose firewall vip virtual-server filter dst-port on page 2886](#)
- [diagnose firewall vip virtual-server filter list on page 2886](#)
- [diagnose firewall vip virtual-server filter name on page 2886](#)
- [diagnose firewall vip virtual-server filter negate on page 2886](#)
- [diagnose firewall vip virtual-server filter negate dst-addr on page 2886](#)
- [diagnose firewall vip virtual-server filter negate dst-port on page 2887](#)
- [diagnose firewall vip virtual-server filter negate name on page 2887](#)
- [diagnose firewall vip virtual-server filter negate src-addr on page 2887](#)
- [diagnose firewall vip virtual-server filter negate src-port on page 2887](#)
- [diagnose firewall vip virtual-server filter negate vd on page 2887](#)
- [diagnose firewall vip virtual-server filter negate worker on page 2887](#)
- [diagnose firewall vip virtual-server filter src on page 2888](#)
- [diagnose firewall vip virtual-server filter src-port on page 2888](#)
- [diagnose firewall vip virtual-server filter vd on page 2888](#)
- [diagnose firewall vip virtual-server filter worker on page 2888](#)
- [diagnose firewall vip virtual-server real-server on page 2889](#)

- [diagnose firewall vip virtual-server real-server list on page 2889](#)
- [diagnose firewall vip virtual-server stats on page 2889](#)
- [diagnose firewall vip virtual-server stats clear on page 2889](#)
- [diagnose firewall vip virtual-server stats crypto-clear on page 2889](#)
- [diagnose firewall vip virtual-server stats http on page 2889](#)
- [diagnose firewall vip virtual-server stats http all on page 2890](#)
- [diagnose firewall vip virtual-server stats http clear on page 2890](#)
- [diagnose firewall vip virtual-server stats http list on page 2890](#)
- [diagnose firewall vip virtual-server stats list on page 2890](#)
- [diagnose firewall vip virtual-server stats operational on page 2890](#)
- [diagnose firewall vip virtual-server stats operational all on page 2890](#)
- [diagnose firewall vip virtual-server stats operational list on page 2891](#)
- [diagnose firewall vip virtual-server stats ssl on page 2891](#)
- [diagnose firewall vip virtual-server stats ssl all on page 2891](#)
- [diagnose firewall vip virtual-server stats ssl clear on page 2891](#)
- [diagnose firewall vip virtual-server stats ssl list on page 2891](#)
- [diagnose firewall vip virtual-server stats summary on page 2891](#)
- [diagnose firewall vip virtual-server stats summary all on page 2892](#)
- [diagnose firewall vip virtual-server stats summary clear on page 2892](#)
- [diagnose firewall vip virtual-server stats summary list on page 2892](#)
- [diagnose firewall vip virtual-server test on page 2892](#)
- [diagnose firewall vip virtual-server test benchmark on page 2892](#)
- [diagnose firewall vip virtual-server test benchmark dh-make-key on page 2892](#)
- [diagnose firewall vip virtual-server test benchmark dh-make-secret on page 2893](#)
- [diagnose firewall vip virtual-server test benchmark rand on page 2893](#)
- [diagnose firewall vip virtual-server test benchmark rsa on page 2893](#)
- [diagnose firewall vip virtual-server test benchmark rsa-mskb on page 2893](#)
- [diagnose firewall vip virtual-server test key-exchange on page 2893](#)
- [diagnose firewall vip virtual-server test key-exchange async on page 2893](#)
- [diagnose firewall vip virtual-server test key-exchange sync on page 2894](#)
- [diagnose firewall vip virtual-server test next-proto on page 2894](#)
- [diagnose firewall vip virtual-server test next-proto disable on page 2894](#)
- [diagnose firewall vip virtual-server test next-proto enable on page 2894](#)
- [diagnose firewall vip virtual-server test rsa-blinding on page 2894](#)
- [diagnose firewall vip virtual-server test rsa-blinding disable on page 2894](#)
- [diagnose firewall vip virtual-server test rsa-blinding enable on page 2895](#)
- [diagnose firewall vip virtual-server test ssl on page 2895](#)
- [diagnose firewall vip virtual-server test ssl async on page 2895](#)
- [diagnose firewall vip virtual-server test ssl sync on page 2895](#)

diagnose firewall auth

Authenticated users.

```
diagnose firewall auth
```

diagnose firewall auth clear

Clear authenticated IPv4 users.

```
diagnose firewall auth clear
```

diagnose firewall auth filter

Filters used to list entries.

```
diagnose firewall auth filter
```

diagnose firewall auth filter clear

Clear all filters.

```
diagnose firewall auth filter clear
```

diagnose firewall auth filter group

Group name.

```
diagnose firewall auth filter group <name>
```

Parameter	Description	Type	Size
<name>	Group name.	string	

diagnose firewall auth filter mac

MAC address.

```
diagnose firewall auth filter mac <xx:xx:xx:xx:xx:xx>
```

Parameter	Description	Type	Size
<xx:xx:xx:xx:xx:xx>	MAC address.	string	

diagnose firewall auth filter method

method

```
diagnose firewall auth filter method <method> <method> <method> <method> <method> <method>
```

Parameter	Description	Type	Size
<method>	Valid method name: fsso, rsso, ntlm, fw, wsso, disclaimer, fsso_citrix, sso_guest.	string	
<method>	Valid method name: fsso, rsso, ntlm, fw, wsso, email, disclaimer, fsso_citrix, sso_guest.	string	
<method>	Valid method name: fsso, rsso, ntlm, fw, wsso, email, disclaimer, fsso_citrix, sso_guest.	string	
<method>	Valid method name: fsso, rsso, ntlm, fw, wsso, email, disclaimer, fsso_citrix, sso_guest.	string	
<method>	Valid method name: fsso, rsso, ntlm, fw, wsso, email, disclaimer, fsso_citrix, sso_guest.	string	
<method>	Valid method name: fsso, rsso, ntlm, fw, wsso, email, disclaimer, fsso_citrix, sso_guest.	string	

diagnose firewall auth filter policy

Policy ID.

```
diagnose firewall auth filter policy <xxx>
```

Parameter	Description	Type	Size
<xxx>	Policy ID.	string	

diagnose firewall auth filter source

IPv4 source address.

```
diagnose firewall auth filter source <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	IPv4 source (range from).	string	
<xxx.xxx.xxx.xxx>	IPv4 source (range to).	string	

diagnose firewall auth filter source6

IPv6 source address.

```
diagnose firewall auth filter source6 <xxxx::xxx> <xxxx::xxx>
```

Parameter	Description	Type	Size
<xxxx::xxx>	IPv6 source (range from).	string	
<xxxx::xxx>	IPv6 source (range to).	string	

diagnose firewall auth filter user

User name.

```
diagnose firewall auth filter user <name>
```

Parameter	Description	Type	Size
<name>	User name.	string	

diagnose firewall auth ipv6

Authenticated IPv6 users.

```
diagnose firewall auth ipv6
```

diagnose firewall auth ipv6 clear

Clear authenticated IPv6 users.

```
diagnose firewall auth ipv6 clear
```

diagnose firewall auth ipv6 list

List authenticated IPv6 users.

```
diagnose firewall auth ipv6 list
```

diagnose firewall auth list

List authenticated IPv4 users.

```
diagnose firewall auth list
```

diagnose firewall auth mac

Authenticated MAC users.

```
diagnose firewall auth mac
```

diagnose firewall auth mac clear

Clear authenticated MAC users.

```
diagnose firewall auth mac clear
```

diagnose firewall auth mac list

List authenticated MAC users.

```
diagnose firewall auth mac list
```

diagnose firewall blocking

Blocking information.

```
diagnose firewall blocking
```


diagnose firewall blocking list

List information.

```
diagnose firewall blocking list <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP.	string	

diagnose firewall dns-xlate

DNS translation.

```
diagnose firewall dns-xlate
```

diagnose firewall dns-xlate mapping

DNS translation mapping.

```
diagnose firewall dns-xlate mapping
```

diagnose firewall dns-xlate mapping list

List dynamic DNS mapping.

```
diagnose firewall dns-xlate mapping list
```

diagnose firewall dns-xlate pool

DNS translation pool.

```
diagnose firewall dns-xlate pool
```

diagnose firewall dns-xlate pool list

List DNS translation pool.

```
diagnose firewall dns-xlate pool list
```

diagnose firewall dynamic

Show dynamic addresses.

```
diagnose firewall dynamic
```

diagnose firewall dynamic address

Get summary of one or all dynamic addresses.

```
diagnose firewall dynamic address <name>
```

Parameter	Description	Type	Size
<name>	Dynamic address name. (Optional)	string	

diagnose firewall dynamic list

Get list of one or all dynamic addresses.

```
diagnose firewall dynamic list <name>
```

Parameter	Description	Type	Size
<name>	Dynamic address name. (Optional)	string	

diagnose firewall dynamic test-common-tag-update

Test update tags API for dynamic addresses.

```
diagnose firewall dynamic test-common-tag-update <TAG-INFO-JSON>
```

Parameter	Description	Type	Size
<TAG-INFO-JSON>	JSON string for commands.	string	

diagnose firewall dynamic6

Show IPv6 dynamic addresses.

```
diagnose firewall dynamic6
```

diagnose firewall dynamic6 address

Get summary of IPv6 dynamic addresses.

```
diagnose firewall dynamic6 address <name>
```

Parameter	Description	Type	Size
<name>	Dynamic address name.	string	

diagnose firewall dynamic6 list

List all IPv6 dynamic addresses.

```
diagnose firewall dynamic6 list <name>
```

Parameter	Description	Type	Size
<name>	Dynamic address name.	string	

diagnose firewall fqdn

fqdn

```
diagnose firewall fqdn
```

diagnose firewall fqdn get-ip

Get and display one IP FQDN address.

```
diagnose firewall fqdn get-ip <name>
```

Parameter	Description	Type	Size
<name>	Address Name	string	

diagnose firewall fqdn get-mac

Get and display one MAC FQDN address.

```
diagnose firewall fqdn get-mac <name>
```

Parameter	Description	Type	Size
<name>	Address Name	string	

diagnose firewall fqdn getinfo-ip

Get info of IP FQDN address

```
diagnose firewall fqdn getinfo-ip <name>
```

Parameter	Description	Type	Size
<name>	name	string	

diagnose firewall fqdn getinfo-mac

Get info of MAC FQDN address

```
diagnose firewall fqdn getinfo-mac <name>
```

Parameter	Description	Type	Size
<name>	name	string	

diagnose firewall fqdn list-all

List FQDN.

```
diagnose firewall fqdn list-all
```

diagnose firewall fqdn list-ip

List IP FQDN.

```
diagnose firewall fqdn list-ip
```

diagnose firewall fqdn list-mac

List MAC FQDN.

```
diagnose firewall fqdn list-mac
```

diagnose firewall fqdn6

IPv6 FQDN.

```
diagnose firewall fqdn6
```

diagnose firewall fqdn6 list

List all IPv6 FQDN.

```
diagnose firewall fqdn6 list
```

diagnose firewall internet-service

Internet service in the kernel.

```
diagnose firewall internet-service
```

diagnose firewall internet-service list

List Internet Service.

```
diagnose firewall internet-service list <section>
```

Parameter	Description	Type	Size
<section>	Internet Service table section.(0: entry, 1: index, <integer>: singularity)	string	

diagnose firewall internet-service-app-ctrl

Application control internet service in the kernel.

```
diagnose firewall internet-service-app-ctrl
```

diagnose firewall internet-service-app-ctrl list

List application control entries in the kernel.

```
diagnose firewall internet-service-app-ctrl list <ID>
```

Parameter	Description	Type	Size
<ID>	Application Control ID.	string	

diagnose firewall internet-service-app-ctrl6

Application control internet service for IPv6 in the kernel.

```
diagnose firewall internet-service-app-ctrl6
```

diagnose firewall internet-service-app-ctrl6 list

List IPv6 application control entries in the kernel.

```
diagnose firewall internet-service-app-ctrl6 list <ID>
```

Parameter	Description	Type	Size
<ID>	Application Control ID.	string	

diagnose firewall internet-service-cache

Internet Service database cache entries in the kernel.

```
diagnose firewall internet-service-cache
```

diagnose firewall internet-service-cache list

List Internet Service database cache entries in the kernel.

```
diagnose firewall internet-service-cache list
```

diagnose firewall internet-service-custom

Custom Internet Service in the kernel.

```
diagnose firewall internet-service-custom
```

diagnose firewall internet-service-custom list

List Custom Internet Service.

```
diagnose firewall internet-service-custom list <name>
```

Parameter	Description	Type	Size
<name>	Custom Internet Service name.	string	

diagnose firewall internet-service-disable

Internet Service disable entries in the kernel.

```
diagnose firewall internet-service-disable
```

diagnose firewall internet-service-disable list

List Internet Service disable entries.

```
diagnose firewall internet-service-disable list <ID>
```

Parameter	Description	Type	Size
<ID>	Internet Service ID.	string	

diagnose firewall internet-service-extension

Internet Service extension in the kernel.

```
diagnose firewall internet-service-extension
```

diagnose firewall internet-service-extension list

List Internet Service extension.

```
diagnose firewall internet-service-extension list <ID>
```

Parameter	Description	Type	Size
<ID>	Internet Service ID.	string	

diagnose firewall internet-service-prio-id

Internet service ID in firewall policy, shaping policy, SD-WAN rule, static route, and router policy.

```
diagnose firewall internet-service-prio-id
```

diagnose firewall internet-service-prio-id list

List Internet Service Priority ID.

```
diagnose firewall internet-service-prio-id list
```

diagnose firewall internet-service6

Internet service6 in the kernel.

```
diagnose firewall internet-service6
```

diagnose firewall internet-service6 list

List Internet Service6.

```
diagnose firewall internet-service6 list <section>
```

Parameter	Description	Type	Size
<section>	Internet Service6 table section.(0: entry, 1: index, <integer>: singularity)	string	

diagnose firewall internet-service6-cache

Internet Service database cache entries for IPv6 in the kernel.

```
diagnose firewall internet-service6-cache
```

diagnose firewall internet-service6-cache list

List Internet Service database cache entries for IPv6 in the kernel.

```
diagnose firewall internet-service6-cache list
```


diagnose firewall internet-service6-custom

Custom Internet Service6 in the kernel.

```
diagnose firewall internet-service6-custom
```

diagnose firewall internet-service6-custom list

List Custom Internet Service.

```
diagnose firewall internet-service6-custom list <name>
```

Parameter	Description	Type	Size
<name>	Custom Internet Service name.	string	

diagnose firewall internet-service6-disable

Internet Service6 disable entries in the kernel.

```
diagnose firewall internet-service6-disable
```

diagnose firewall internet-service6-disable list

List Internet Service6 disable entries.

```
diagnose firewall internet-service6-disable list <ID>
```

Parameter	Description	Type	Size
<ID>	Internet Service6 ID.	string	

diagnose firewall internet-service6-extension

Internet Service6 extension in the kernel.

```
diagnose firewall internet-service6-extension
```

diagnose firewall internet-service6-extension list

List Internet Service6 extension.

```
diagnose firewall internet-service6-extension list <ID>
```

Parameter	Description	Type	Size
<ID>	Internet Service6 ID.	string	

diagnose firewall internet-service6-prio-id

Internet service ID in firewall policy, SD-WAN rule, and router policy.

```
diagnose firewall internet-service6-prio-id
```

diagnose firewall internet-service6-prio-id list

List Internet Service6 Priority ID.

```
diagnose firewall internet-service6-prio-id list
```

diagnose firewall ip-translation

IP translation.

```
diagnose firewall ip-translation
```

diagnose firewall ip-translation list

List IP translation table.

```
diagnose firewall ip-translation list
```

diagnose firewall ipgeo

IP geolocation.

```
diagnose firewall ipgeo
```

diagnose firewall ipgeo copyright-notice

Copyright note.

```
diagnose firewall ipgeo copyright-notice
```

diagnose firewall ipgeo country-list

List all countries.

```
diagnose firewall ipgeo country-list
```

diagnose firewall ipgeo ip-list

List IP info of country.

```
diagnose firewall ipgeo ip-list <name>
```

Parameter	Description	Type	Size
<name>	Country ID.	string	

diagnose firewall ipgeo ip2country

Get country info for the IP.

```
diagnose firewall ipgeo ip2country <ip>
```

Parameter	Description	Type	Size
<ip>	IPv4/IPv6 address.	string	

diagnose firewall ipgeo ip6-list

List IPv6 info of country.

```
diagnose firewall ipgeo ip6-list <name>
```

Parameter	Description	Type	Size
<name>	Country ID.	string	

diagnose firewall ipgeo override

Print out all user defined IP geolocation data.

```
diagnose firewall ipgeo override
```

diagnose firewall iplist

IP list.

```
diagnose firewall iplist
```

diagnose firewall iplist list

list

```
diagnose firewall iplist list
```

diagnose firewall iplist list optimized

List optimized iplist.

```
diagnose firewall iplist list optimized
```

diagnose firewall iplist6

IPv6 list.

```
diagnose firewall iplist6
```

diagnose firewall iplist6 list

list

```
diagnose firewall iplist6 list
```

diagnose firewall iplist6 list optimized

List optimized iplist6.

```
diagnose firewall iplist6 list optimized
```

diagnose firewall ipmac

ipmac

```
diagnose firewall ipmac
```

diagnose firewall ipmac add

add

```
diagnose firewall ipmac add <xxx.xxx.xxx.xxx> <xx:xx:xx:xx:xx:xx> <drop|accept>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	IP address.	string	
<xx:xx:xx:xx:xx:xx>	MAC address.	string	
<drop accept>	action	string	

diagnose firewall ipmac delete

delete

```
diagnose firewall ipmac delete <xxx.xxx.xxx.xxx> <xx:xx:xx:xx:xx:xx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	IP address.	string	
<xx:xx:xx:xx:xx:xx>	MAC address.	string	

diagnose firewall ipmac list

list

```
diagnose firewall ipmac list
```

diagnose firewall ipmac status

status

```
diagnose firewall ipmac status
```

diagnose firewall ippool

One-to-one/PBA IP pool.

```
diagnose firewall ippool
```

diagnose firewall ippool filter

Diag ippool list with filters.

```
diagnose firewall ippool filter
```

diagnose firewall ippool filter clear

Clear diag ippool filter.

```
diagnose firewall ippool filter clear
```

diagnose firewall ippool filter name

Ippool pool name.

```
diagnose firewall ippool filter name
```

diagnose firewall ippool list

list

```
diagnose firewall ippool list
```

diagnose firewall ippool list nat-ip

List allocated IP in ippool. Take ippool names as arguments.

```
diagnose firewall ippool list nat-ip
```

diagnose firewall ippool list pba

List PBA in ippool. Take ippool names as arguments.

```
diagnose firewall ippool list pba
```

diagnose firewall ippool list user

List users of ippool. Take ippool names as arguments.

```
diagnose firewall ippool list user
```

diagnose firewall ippool reset-log-stats

reset log statistics

```
diagnose firewall ippool reset-log-stats
```

diagnose firewall ippool stats

statistics

```
diagnose firewall ippool stats
```

diagnose firewall ippool-all

Any IP pool.

```
diagnose firewall ippool-all
```

diagnose firewall ippool-all list

list

```
diagnose firewall ippool-all list
```

diagnose firewall ippool-all stats

statistics

```
diagnose firewall ippool-all stats <name>
```

Parameter	Description	Type	Size
<name>	pool name	string	

diagnose firewall ippool-fixed-range

Fixed range IP pool.

```
diagnose firewall ippool-fixed-range
```

diagnose firewall ippool-fixed-range list

list

```
diagnose firewall ippool-fixed-range list
```

diagnose firewall ippool-fixed-range list natip

NAT IP.

```
diagnose firewall ippool-fixed-range list natip <xxx.xxx.xxx.xxx>[-<xxx.xxx.xxx.xxx>]  
<Enter>|<port>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>[-<xxx.xxx.xxx.xxx>]	NAT IP/IP range NAT IP/IP Range + port.	string	
<Enter> <port>	port	string	

diagnose firewall ippool-nptv6

NPTv6 IP pool.

```
diagnose firewall ippool-nptv6
```

diagnose firewall ippool-nptv6 natip

NAT IPV6.

```
diagnose firewall ippool-nptv6 natip <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>
```

Parameter	Description	Type	Size
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>	NAT IPV6.	string	

diagnose firewall iprope

iprope

```
diagnose firewall iprope
```

diagnose firewall iprope appctrl

List application control lists.

```
diagnose firewall iprope appctrl
```

diagnose firewall iprope appctrl list

List application control lists.

```
diagnose firewall iprope appctrl list
```

diagnose firewall iprope appctrl shaper

application control app shapers.

```
diagnose firewall iprope appctrl shaper
```

diagnose firewall iprope appctrl shaper list

List application control app shapers.

```
diagnose firewall iprope appctrl shaper list
```

diagnose firewall iprope appctrl stats

Application control app statistics.

```
diagnose firewall iprope appctrl stats
```

diagnose firewall iprope appctrl stats clear

Clear application control app statistics.

```
diagnose firewall iprope appctrl stats clear
```

diagnose firewall iprope appctrl stats list

List application control app statistics.

```
diagnose firewall iprope appctrl stats list
```

diagnose firewall iprope appctrl status

Application control list status.

```
diagnose firewall iprope appctrl status
```

diagnose firewall iprope clear

Clear policy statistic.

```
diagnose firewall iprope clear
```

diagnose firewall iprope list

List.

```
diagnose firewall iprope list <No.>
```

Parameter	Description	Type	Size
<No.>	Number, hexadecimal.	string	

diagnose firewall iprope lookup

Lookup firewall policy that matches provided criteria.

```
diagnose firewall iprope lookup <src_ip> <src_port> <dst_ip> <dst_port> <protocol> <device> <pol_type> [  
<auth type>] [  
<user/group>] [  
<server>] [  
<user-db>] [  
<group-attr-type>]
```

Parameter	Description	Type	Size
<src_ip>	Source IP address.	string	
<src_port>	Source port.	string	
<dst_ip>	Destination IP address.	string	
<dst_port>	Destination port.	string	
<protocol>	Protocol.	string	
<device>	Source interface.	string	
<pol_type>	Firewall policy type: policy, proxy.	string	
[<auth type>]	Authentication type: ldap, saml, local, group.	string	
[<user/group>]	Username or name of matching user/group on remote authentication server.	string	
[<server>]	Name of auth server.	string	
[<user-db>]	Name of user-database.	string	
[<group-attr-type>]	Group attr type: name, id.	string	

diagnose firewall iprope show

Show policy statistic.

```
diagnose firewall iprope show
```

diagnose firewall iprope state

state

```
diagnose firewall iprope state
```

diagnose firewall iprope top

Show top N policy statistics within a group.

```
diagnose firewall iprope top <No.> <String> <Integer> <Integer> <Integer>
```

Parameter	Description	Type	Size
<No.>	Policy group ID	string	
<String>	Sort by pkts[-rate]/asic-pkts[-rate]/hit-count[-rate]/tcp-ses[-rate]/udp-ses[-rate]/sctp-ses[-rate]/all-ses[-rate].	string	
<Integer>	Delay in seconds (default: 5).	string	
<Integer>	Number of policy statistics to display (default: 10).	string	
<Integer>	Iterations to run (default: unlimited).	string	

diagnose firewall iprope6

iprope6

```
diagnose firewall iprope6
```

diagnose firewall iprope6 clear

Clear policy statistic.

```
diagnose firewall iprope6 clear
```

diagnose firewall iprope6 list

list

```
diagnose firewall iprope6 list <No.>
```

Parameter	Description	Type	Size
<No.>	Number, hexadecimal.	string	

diagnose firewall iprope6 lookup

Lookup firewall policy that matches provided criteria.

```
diagnose firewall iprope6 lookup <src_ip> <src_port> <dst_ip> <dst_port> <protocol> <device> <pol_type> [  
<auth type>] [<user/group>] [<server>]
```

Parameter	Description	Type	Size
<src_ip>	Source IP address.	string	
<src_port>	Source port.	string	
<dst_ip>	Destination IP address.	string	
<dst_port>	Destination port.	string	
<protocol>	Protocol.	string	
<device>	Source interface.	string	
<pol_type>	Firewall policy type: policy, proxy.	string	
[<auth type>]	Authentication type: user, group.	string	
[<user/group>]	Username or name of matching user/group on remote authentication server.	string	
[<server>]	Name of auth server.	string	

diagnose firewall iprope6 show

Show policy statistic.

```
diagnose firewall iprope6 show
```

diagnose firewall iprope6 state

state

```
diagnose firewall iprope6 state
```

diagnose firewall iprope6 top

Show top N policy statistics within a group.

```
diagnose firewall iprope6 top <No.> <String> <Integer> <Integer> <Integer>
```

Parameter	Description	Type	Size
<No.>	Policy group ID	string	
<String>	Sort by pkts[-rate]/asic-pkts[-rate]/hit-count[-rate]/tcp-ses[-rate]/udp-ses[-rate]/sctp-ses[-rate]/all-ses[-rate].	string	
<Integer>	Delay in seconds (default: 5).	string	
<Integer>	Number of policy statistics to display (default: 10, maximum: 50).	string	
<Integer>	Iterations to run (default: unlimited).	string	

diagnose firewall ipv6-ehf

IPv6 extension header filter.

```
diagnose firewall ipv6-ehf
```

diagnose firewall ipv6-ehf list

List ipv6-eh-filter.

```
diagnose firewall ipv6-ehf list
```

diagnose firewall network-service-dynamic

Dynamic Network Service in the kernel.

```
diagnose firewall network-service-dynamic
```

diagnose firewall network-service-dynamic list

List Dynamic Network Service.

```
diagnose firewall network-service-dynamic list <name>
```

Parameter	Description	Type	Size
<name>	Dynamic Network Service name.	string	

diagnose firewall ngfw-fix-application

Next Generation Firewall (NGFW) Applications handled by Kernel.

```
diagnose firewall ngfw-fix-application
```

diagnose firewall ngfw-fix-application list

List Kernel-handled NGFW applications.

```
diagnose firewall ngfw-fix-application list
```

diagnose firewall packet

Packet statistics.

```
diagnose firewall packet
```

diagnose firewall packet distribution

Show distribution statistics.

```
diagnose firewall packet distribution
```

diagnose firewall pcp-mapping

PCP mapping list.

```
diagnose firewall pcp-mapping
```

diagnose firewall pcp-mapping filter

List/flush mapping with filters.

```
diagnose firewall pcp-mapping filter
```

diagnose firewall pcp-mapping filter clear

Clear PCP mapping filter.

```
diagnose firewall pcp-mapping filter clear
```

diagnose firewall pcp-mapping filter client-ip

Client IP address.

```
diagnose firewall pcp-mapping filter client-ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	client IP address (from).	string	
<xxx.xxx.xxx.xxx>	Client IP address IP (to).	string	

diagnose firewall pcp-mapping filter ext-ip

External IP address.

```
diagnose firewall pcp-mapping filter ext-ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	External IP address (from).	string	
<xxx.xxx.xxx.xxx>	External IP address IP (to).	string	

diagnose firewall pcp-mapping filter ext-port

External port.

```
diagnose firewall pcp-mapping filter ext-port <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose firewall pcp-mapping filter intl-ip

Internal IP address.

```
diagnose firewall pcp-mapping filter intl-ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Internal IP address (from).	string	
<xxx.xxx.xxx.xxx>	Internal IP address IP (to).	string	

diagnose firewall pcp-mapping filter intl-port

Internal port.

```
diagnose firewall pcp-mapping filter intl-port <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose firewall pcp-mapping filter pool

Pool ID.

```
diagnose firewall pcp-mapping filter pool <xx>
```

Parameter	Description	Type	Size
<xx>	Pool ID.	string	

diagnose firewall pcp-mapping filter protocol

Protocol number.

```
diagnose firewall pcp-mapping filter protocol <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255>.	string	

diagnose firewall pcp-mapping filter remote-ip

Remote IP address.

```
diagnose firewall pcp-mapping filter remote-ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Remote IP address (from).	string	
<xxx.xxx.xxx.xxx>	Remote IP address IP (to).	string	

diagnose firewall pcp-mapping filter remote-port

Remote port.

```
diagnose firewall pcp-mapping filter remote-port <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose firewall pcp-mapping flush

flush

```
diagnose firewall pcp-mapping flush
```

diagnose firewall pcp-mapping flush inbound

Flush PCP MAP mapping.

```
diagnose firewall pcp-mapping flush inbound
```

diagnose firewall pcp-mapping flush outbound

Flush PCP PEER mapping.

```
diagnose firewall pcp-mapping flush outbound
```

diagnose firewall pcp-mapping list

list

```
diagnose firewall pcp-mapping list
```

diagnose firewall pcp-mapping list inbound

List PCP MAP mapping.

```
diagnose firewall pcp-mapping list inbound
```

diagnose firewall pcp-mapping list outbound

List PCP PEER mapping.

```
diagnose firewall pcp-mapping list outbound
```

diagnose firewall proute

Policy route.

```
diagnose firewall proute
```

diagnose firewall proute clear

Clear policy routing stats.

```
diagnose firewall proute clear <number>
```

Parameter	Description	Type	Size
<number>	Policy route ID.	string	

diagnose firewall proute list

List policy routing.

```
diagnose firewall proute list <number>
```

Parameter	Description	Type	Size
<number>	Policy route ID.	string	

diagnose firewall proute show

Show policy routing stats.

```
diagnose firewall proute show <number>
```

Parameter	Description	Type	Size
<number>	Policy route ID.	string	

diagnose firewall proute6

IPv6 policy route.

```
diagnose firewall proute6
```

diagnose firewall proute6 clear

Clear IPv6 policy routing stats.

```
diagnose firewall proute6 clear <number>
```

Parameter	Description	Type	Size
<number>	Policy route ID.	string	

diagnose firewall proute6 list

List IPv6 policy routing.

```
diagnose firewall proute6 list
```

diagnose firewall proute6 show

Show IPv6 policy routing stats.

```
diagnose firewall proute6 show <number>
```

Parameter	Description	Type	Size
<number>	Policy route ID.	string	

diagnose firewall route_tag

Route tag.

```
diagnose firewall route_tag
```

diagnose firewall route_tag list

List Route tag address.

```
diagnose firewall route_tag list <number>
```

Parameter	Description	Type	Size
<number>	Router tag ID.	string	

diagnose firewall route_tag_v6

route_tag_v6.

```
diagnose firewall route_tag_v6
```

diagnose firewall route_tag_v6 list

List Route tag address v6.

```
diagnose firewall route_tag_v6 list <number>
```

Parameter	Description	Type	Size
<number>	Router tag ID.	string	

diagnose firewall schedule

schedule

```
diagnose firewall schedule
```

diagnose firewall schedule debug

Set policy schedule debug level.

```
diagnose firewall schedule debug <level>
```

Parameter	Description	Type	Size
<level>	debug level (0-2)	string	

diagnose firewall schedule list

List schedule.

```
diagnose firewall schedule list
```

diagnose firewall schedule reload

Reload schedule.

```
diagnose firewall schedule reload
```

diagnose firewall sf-addresses

Security Fabric device addresses.

```
diagnose firewall sf-addresses
```

diagnose firewall sf-addresses list

List IP addresses of Fortinet devices configured in the Security Fabric.

```
diagnose firewall sf-addresses list
```

diagnose firewall shaper

shapers

```
diagnose firewall shaper
```

diagnose firewall shaper dynamic-shaper

Dynamic shapers.

```
diagnose firewall shaper dynamic-shaper
```

diagnose firewall shaper dynamic-shaper flush

Flush all dynamic shapers.

```
diagnose firewall shaper dynamic-shaper flush
```

diagnose firewall shaper dynamic-shaper list

List Dynamic shapers.

```
diagnose firewall shaper dynamic-shaper list
```

diagnose firewall shaper dynamic-shaper list ip

IPv4 address.

```
diagnose firewall shaper dynamic-shaper list ip <IP addr>
```

Parameter	Description	Type	Size
<IP addr>	IPv4 Adress xxx.xxx.xxx.xxx.	string	

diagnose firewall shaper dynamic-shaper list ipv6

IPv6 address.

```
diagnose firewall shaper dynamic-shaper list ipv6 <IPv6 addr>
```

Parameter	Description	Type	Size
<IPv6 addr>	IPv6 Adress xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx	string	

diagnose firewall shaper dynamic-shaper list user

User name.

```
diagnose firewall shaper dynamic-shaper list user <string>
```

Parameter	Description	Type	Size
<string>	User name.	string	

diagnose firewall shaper dynamic-shaper stats

Dynamic shapers statistic.

```
diagnose firewall shaper dynamic-shaper stats
```

diagnose firewall shaper per-ip-shaper

Traffic shapers.

```
diagnose firewall shaper per-ip-shaper
```

diagnose firewall shaper per-ip-shaper clear

Per-IP clear statistic data.

```
diagnose firewall shaper per-ip-shaper clear
```

diagnose firewall shaper per-ip-shaper list

List per-IP shapers.

```
diagnose firewall shaper per-ip-shaper list
```

diagnose firewall shaper per-ip-shaper state

Per-IP shapers state.

```
diagnose firewall shaper per-ip-shaper state
```


diagnose firewall shaper per-ip-shaper stats

Per-IP shapers statistic.

```
diagnose firewall shaper per-ip-shaper stats
```

diagnose firewall shaper traffic-shaper

Traffic shapers.

```
diagnose firewall shaper traffic-shaper
```

diagnose firewall shaper traffic-shaper list

List traffic shapers.

```
diagnose firewall shaper traffic-shaper list
```

diagnose firewall shaper traffic-shaper state

Global traffic shaper state.

```
diagnose firewall shaper traffic-shaper state
```

diagnose firewall shaper traffic-shaper stats

Traffic shaper statistics.

```
diagnose firewall shaper traffic-shaper stats
```

diagnose firewall shaper traffic-shaper stats clear

Clear traffic shaper statistics.

```
diagnose firewall shaper traffic-shaper stats clear <name>
```

Parameter	Description	Type	Size
<name>	Name of traffic shaper to clear.	string	

diagnose firewall shaper traffic-shaper stats list

List traffic shaper statistics.

```
diagnose firewall shaper traffic-shaper stats list
```

diagnose firewall uuid

UUID list.

```
diagnose firewall uuid
```

diagnose firewall uuid list

list

```
diagnose firewall uuid list <type>
```

Parameter	Description	Type	Size
<type>	UUID category.	string	

diagnose firewall vendor-mac

Vendor MAC in the kernel.

```
diagnose firewall vendor-mac
```

diagnose firewall vendor-mac list

List Vendor MAC Entries.

```
diagnose firewall vendor-mac list
```

diagnose firewall vip

VIP diagnostics.

```
diagnose firewall vip
```

diagnose firewall vip realserver

Load balance real servers.

```
diagnose firewall vip realserver
```

diagnose firewall vip realserver clear

Clear firewall VIP, VIP6 real server statistics.

```
diagnose firewall vip realserver clear
```

diagnose firewall vip realserver clear vip

Clear VIP real server statistics.

```
diagnose firewall vip realserver clear vip <name> <IPv4|IPv6|all>
```

Parameter	Description	Type	Size
<name>	firewall VIP name.	string	
<IPv4 IPv6 all>	IPv4 address x.x.x.x or IPv6 address x:x:x:x:x:x of the real server, use "all" to clear statistics of all real servers of this VIP.	string	

diagnose firewall vip realserver clear vip6

Clear VIP6 real server statistics.

```
diagnose firewall vip realserver clear vip6 <name> <IPv4|IPv6|all>
```

Parameter	Description	Type	Size
<name>	Firewall VIP6 name.	string	
<IPv4 IPv6 all>	IPv4 address x.x.x.x or IPv6 address x:x:x:x:x:x of the real server, use "all" to clear statistics of all real servers of this VIP6.	string	

diagnose firewall vip realserver down

Change address down.

```
diagnose firewall vip realserver down <name> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<name>	IP address.	string	
<xxx.xxx.xxx.xxx>	IP address.	string	

diagnose firewall vip realserver healthcheck

Server health check.

```
diagnose firewall vip realserver healthcheck
```

diagnose firewall vip realserver healthcheck stats

Health check statistics.

```
diagnose firewall vip realserver healthcheck stats
```

diagnose firewall vip realserver healthcheck stats clear

Clear health check statistics.

```
diagnose firewall vip realserver healthcheck stats clear
```

diagnose firewall vip realserver healthcheck stats show

Show health check statistics.

```
diagnose firewall vip realserver healthcheck stats show
```

diagnose firewall vip realserver list

list

```
diagnose firewall vip realserver list
```

diagnose firewall vip realserver up

Change address up.

```
diagnose firewall vip realserver up <name> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<name>	IP address.	string	
<xxx.xxx.xxx.xxx>	IP address.	string	

diagnose firewall vip virtual-server

Virtual-server diagnostics.

```
diagnose firewall vip virtual-server
```

diagnose firewall vip virtual-server filter

Filter for various virtual server diagnostics.

```
diagnose firewall vip virtual-server filter
```

diagnose firewall vip virtual-server filter clear

Erase the current filter.

```
diagnose firewall vip virtual-server filter clear
```

diagnose firewall vip virtual-server filter dst

Destination address range to filter by.

```
diagnose firewall vip virtual-server filter dst <ip-address> <ip-address>
```

Parameter	Description	Type	Size
<ip-address>	Destination IP address (from).	string	
<ip-address>	Destination IP address (to).	string	

diagnose firewall vip virtual-server filter dst-port

Destination port range to filter by.

```
diagnose firewall vip virtual-server filter dst-port <port> <port>
```

Parameter	Description	Type	Size
<port>	Destination port (from).	string	
<port>	Destination port (to).	string	

diagnose firewall vip virtual-server filter list

Display the current filter.

```
diagnose firewall vip virtual-server filter list
```

diagnose firewall vip virtual-server filter name

VIP name to filter by.

```
diagnose firewall vip virtual-server filter name <name>
```

Parameter	Description	Type	Size
<name>	Name to filter by.	string	

diagnose firewall vip virtual-server filter negate

Negate the specified filter parameter.

```
diagnose firewall vip virtual-server filter negate
```

diagnose firewall vip virtual-server filter negate dst-addr

Negate IPv4 destination address.

```
diagnose firewall vip virtual-server filter negate dst-addr
```

diagnose firewall vip virtual-server filter negate dst-port

Negate destination port.

```
diagnose firewall vip virtual-server filter negate dst-port
```

diagnose firewall vip virtual-server filter negate name

Negate name.

```
diagnose firewall vip virtual-server filter negate name
```

diagnose firewall vip virtual-server filter negate src-addr

Negate IPv4 source address.

```
diagnose firewall vip virtual-server filter negate src-addr
```

diagnose firewall vip virtual-server filter negate src-port

Negate source port.

```
diagnose firewall vip virtual-server filter negate src-port
```

diagnose firewall vip virtual-server filter negate vd

Negate virtual domain.

```
diagnose firewall vip virtual-server filter negate vd
```

diagnose firewall vip virtual-server filter negate worker

Negate worker index.

```
diagnose firewall vip virtual-server filter negate worker
```

diagnose firewall vip virtual-server filter src

Source address range to filter by.

```
diagnose firewall vip virtual-server filter src <ip-address> <ip-address>
```

Parameter	Description	Type	Size
<ip-address>	Source IP address (from).	string	
<ip-address>	Source IP address (to).	string	

diagnose firewall vip virtual-server filter src-port

Source port range to filter by.

```
diagnose firewall vip virtual-server filter src-port <port> <port>
```

Parameter	Description	Type	Size
<port>	Source port (from).	string	
<port>	Source port (to).	string	

diagnose firewall vip virtual-server filter vd

Index of virtual domain. -1 matches all.

```
diagnose firewall vip virtual-server filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose firewall vip virtual-server filter worker

Index of worker. -1 matches all.

```
diagnose firewall vip virtual-server filter worker <index>
```

Parameter	Description	Type	Size
<index>	Index of worker. -1 matches all.	string	

diagnose firewall vip virtual-server real-server

Real-server diagnostics.

```
diagnose firewall vip virtual-server real-server
```

diagnose firewall vip virtual-server real-server list

List servers.

```
diagnose firewall vip virtual-server real-server list
```

diagnose firewall vip virtual-server stats

Statistics.

```
diagnose firewall vip virtual-server stats
```

diagnose firewall vip virtual-server stats clear

Clear all statistics.

```
diagnose firewall vip virtual-server stats clear
```

diagnose firewall vip virtual-server stats crypto-clear

Clear SSL crypto statistics.

```
diagnose firewall vip virtual-server stats crypto-clear
```

diagnose firewall vip virtual-server stats http

HTTP statistics.

```
diagnose firewall vip virtual-server stats http
```

diagnose firewall vip virtual-server stats http all

Per-process HTTP statistics.

```
diagnose firewall vip virtual-server stats http all
```

diagnose firewall vip virtual-server stats http clear

Clear HTTP statistics.

```
diagnose firewall vip virtual-server stats http clear
```

diagnose firewall vip virtual-server stats http list

List HTTP statistics.

```
diagnose firewall vip virtual-server stats http list
```

diagnose firewall vip virtual-server stats list

List all statistics.

```
diagnose firewall vip virtual-server stats list
```

diagnose firewall vip virtual-server stats operational

Operational info and statistics.

```
diagnose firewall vip virtual-server stats operational
```

diagnose firewall vip virtual-server stats operational all

Display per-process operational info and statistics.

```
diagnose firewall vip virtual-server stats operational all
```

diagnose firewall vip virtual-server stats operational list

Display operational info and statistics.

```
diagnose firewall vip virtual-server stats operational list
```

diagnose firewall vip virtual-server stats ssl

SSL statistics.

```
diagnose firewall vip virtual-server stats ssl
```

diagnose firewall vip virtual-server stats ssl all

Per-process SSL statistics.

```
diagnose firewall vip virtual-server stats ssl all
```

diagnose firewall vip virtual-server stats ssl clear

Clear SSL statistics.

```
diagnose firewall vip virtual-server stats ssl clear
```

diagnose firewall vip virtual-server stats ssl list

List SSL statistics.

```
diagnose firewall vip virtual-server stats ssl list
```

diagnose firewall vip virtual-server stats summary

Summary statistics.

```
diagnose firewall vip virtual-server stats summary
```

diagnose firewall vip virtual-server stats summary all

Per-process summary statistics.

```
diagnose firewall vip virtual-server stats summary all
```

diagnose firewall vip virtual-server stats summary clear

Clear summary statistics.

```
diagnose firewall vip virtual-server stats summary clear
```

diagnose firewall vip virtual-server stats summary list

List summary statistics.

```
diagnose firewall vip virtual-server stats summary list
```

diagnose firewall vip virtual-server test

Tests for internal use.

```
diagnose firewall vip virtual-server test
```

diagnose firewall vip virtual-server test benchmark

Crypto performance tests.

```
diagnose firewall vip virtual-server test benchmark
```

diagnose firewall vip virtual-server test benchmark dh-make-key

DH make-key.

```
diagnose firewall vip virtual-server test benchmark dh-make-key
```

diagnose firewall vip virtual-server test benchmark dh-make-secret

DH make-key & make-secret.

```
diagnose firewall vip virtual-server test benchmark dh-make-secret
```

diagnose firewall vip virtual-server test benchmark rand

RAND.

```
diagnose firewall vip virtual-server test benchmark rand
```

diagnose firewall vip virtual-server test benchmark rsa

RSA decryption.

```
diagnose firewall vip virtual-server test benchmark rsa
```

diagnose firewall vip virtual-server test benchmark rsa-mskb

RSA decrypt & MSKB.

```
diagnose firewall vip virtual-server test benchmark rsa-mskb
```

diagnose firewall vip virtual-server test key-exchange

Use synchronous/asynchronous key-exchange.

```
diagnose firewall vip virtual-server test key-exchange
```

diagnose firewall vip virtual-server test key-exchange async

Asynchronous key-exchange.

```
diagnose firewall vip virtual-server test key-exchange async
```

diagnose firewall vip virtual-server test key-exchange sync

Synchronous key-exchange (default).

```
diagnose firewall vip virtual-server test key-exchange sync
```

diagnose firewall vip virtual-server test next-proto

Enable/disable next-proto negotiation.

```
diagnose firewall vip virtual-server test next-proto
```

diagnose firewall vip virtual-server test next-proto disable

Disable next-proto negotiation.

```
diagnose firewall vip virtual-server test next-proto disable
```

diagnose firewall vip virtual-server test next-proto enable

Enable next-proto negotiation.

```
diagnose firewall vip virtual-server test next-proto enable
```

diagnose firewall vip virtual-server test rsa-blinding

Enable/disable RSA blinding.

```
diagnose firewall vip virtual-server test rsa-blinding
```

diagnose firewall vip virtual-server test rsa-blinding disable

Disable RSA blinding.

```
diagnose firewall vip virtual-server test rsa-blinding disable
```

diagnose firewall vip virtual-server test rsa-blinding enable

Enable RSA blinding (default).

```
diagnose firewall vip virtual-server test rsa-blinding enable
```

diagnose firewall vip virtual-server test ssl

SSL.

```
diagnose firewall vip virtual-server test ssl
```

diagnose firewall vip virtual-server test ssl async

Asynchronous SSL (default).

```
diagnose firewall vip virtual-server test ssl async
```

diagnose firewall vip virtual-server test ssl sync

Synchronous SSL.

```
diagnose firewall vip virtual-server test ssl sync
```

diagnose forticare

FortiCare Service.

This topic includes the following commands:

- [diagnose forticare cnreg-code-list on page 2896](#)
- [diagnose forticare direct-registration on page 2896](#)
- [diagnose forticare direct-registration country-data on page 2896](#)
- [diagnose forticare direct-registration organization-list on page 2896](#)
- [diagnose forticare direct-registration product-deregister on page 2896](#)
- [diagnose forticare direct-registration product-registration on page 2897](#)
- [diagnose forticare direct-registration product-transfer on page 2897](#)
- [diagnose forticare direct-registration reseller-list on page 2897](#)

diagnose forticare cnreg-code-list

List known ISO 3166-1 numeric country/region codes.

```
diagnose forticare cnreg-code-list
```

diagnose forticare direct-registration

Direct registration port.

```
diagnose forticare direct-registration
```

diagnose forticare direct-registration country-data

Country data operation.

```
diagnose forticare direct-registration country-data <cnreg-code>
```

Parameter	Description	Type	Size
<cnreg-code>	ISO 3166-1 numeric country/region code.	string	

diagnose forticare direct-registration organization-list

Organization list operation.

```
diagnose forticare direct-registration organization-list
```

diagnose forticare direct-registration product-deregister

Unit deregistration operation.

```
diagnose forticare direct-registration product-deregister <accountID> <password>
```

Parameter	Description	Type	Size
<accountID>	FortiCare user account ID.	string	
<password>	FortiCare user account password.	string	

diagnose forticare direct-registration product-registration

Product registration operation.

```
diagnose forticare direct-registration product-registration
```

diagnose forticare direct-registration product-transfer

Product transfer operation.

```
diagnose forticare direct-registration product-transfer <old-accountID> <password> <new-accountID>  
<password> <is-government>
```

Parameter	Description	Type	Size
<old-accountID>	Old user account ID.	string	
<password>	Old user account password.	string	
<new-accountID>	New user account ID.	string	
<password>	New user account password.	string	
<is-government>	[yes/no]	string	

diagnose forticare direct-registration reseller-list

Reseller list operation.

```
diagnose forticare direct-registration reseller-list <cnreg-code>
```

Parameter	Description	Type	Size
<cnreg-code>	ISO 3166-1 numeric country/region code.	string	

diagnose fortiguard-resources

FortiGuard resources.

This topic includes the following commands:

- [diagnose fortiguard-resources delete on page 2899](#)
- [diagnose fortiguard-resources delete app-categories on page 2899](#)
- [diagnose fortiguard-resources delete app-info on page 2899](#)

- [diagnose fortiguard-resources delete dlp-object on page 2900](#)
- [diagnose fortiguard-resources delete fortiap-end-of-support on page 2900](#)
- [diagnose fortiguard-resources delete fortitxtender-end-of-support on page 2900](#)
- [diagnose fortiguard-resources delete fortigate-end-of-support on page 2900](#)
- [diagnose fortiguard-resources delete fortiswitch-end-of-support on page 2901](#)
- [diagnose fortiguard-resources delete ips-information on page 2901](#)
- [diagnose fortiguard-resources delete prefix-links on page 2901](#)
- [diagnose fortiguard-resources delete sprite-casb on page 2901](#)
- [diagnose fortiguard-resources delete sprite-isdb on page 2901](#)
- [diagnose fortiguard-resources delete sprite-map on page 2901](#)
- [diagnose fortiguard-resources delete static-links on page 2902](#)
- [diagnose fortiguard-resources delete wf-categories on page 2902](#)
- [diagnose fortiguard-resources delete-all on page 2902](#)
- [diagnose fortiguard-resources downloads on page 2902](#)
- [diagnose fortiguard-resources downloads disable on page 2902](#)
- [diagnose fortiguard-resources downloads enable on page 2902](#)
- [diagnose fortiguard-resources info on page 2903](#)
- [diagnose fortiguard-resources info app-categories on page 2903](#)
- [diagnose fortiguard-resources info app-info on page 2903](#)
- [diagnose fortiguard-resources info dlp-object on page 2903](#)
- [diagnose fortiguard-resources info fortiap-end-of-support on page 2903](#)
- [diagnose fortiguard-resources info fortitxtender-end-of-support on page 2904](#)
- [diagnose fortiguard-resources info fortigate-end-of-support on page 2904](#)
- [diagnose fortiguard-resources info fortiswitch-end-of-support on page 2904](#)
- [diagnose fortiguard-resources info ips-information on page 2904](#)
- [diagnose fortiguard-resources info prefix-links on page 2904](#)
- [diagnose fortiguard-resources info sprite-casb.css on page 2905](#)
- [diagnose fortiguard-resources info sprite-casb.png on page 2905](#)
- [diagnose fortiguard-resources info sprite-isdb.css on page 2905](#)
- [diagnose fortiguard-resources info sprite-isdb.png on page 2905](#)
- [diagnose fortiguard-resources info sprite-map.css on page 2905](#)
- [diagnose fortiguard-resources info sprite-map.png on page 2905](#)
- [diagnose fortiguard-resources info static-links on page 2906](#)
- [diagnose fortiguard-resources info wf-categories on page 2906](#)
- [diagnose fortiguard-resources log on page 2906](#)
- [diagnose fortiguard-resources log all on page 2906](#)
- [diagnose fortiguard-resources log app-categories on page 2906](#)
- [diagnose fortiguard-resources log app-info on page 2906](#)
- [diagnose fortiguard-resources log fortiap-end-of-support on page 2907](#)
- [diagnose fortiguard-resources log fortitxtender-end-of-support on page 2907](#)
- [diagnose fortiguard-resources log fortigate-end-of-support on page 2907](#)
- [diagnose fortiguard-resources log fortiswitch-end-of-support on page 2907](#)
- [diagnose fortiguard-resources log ips-information on page 2907](#)

- [diagnose fortiguard-resources log maintainer on page 2907](#)
- [diagnose fortiguard-resources log prefix-links on page 2908](#)
- [diagnose fortiguard-resources log sprite-casb on page 2908](#)
- [diagnose fortiguard-resources log sprite-isdb on page 2908](#)
- [diagnose fortiguard-resources log sprite-map on page 2908](#)
- [diagnose fortiguard-resources log static-links on page 2908](#)
- [diagnose fortiguard-resources log wf-categories on page 2908](#)
- [diagnose fortiguard-resources update on page 2909](#)
- [diagnose fortiguard-resources update app-categories on page 2909](#)
- [diagnose fortiguard-resources update app-info on page 2909](#)
- [diagnose fortiguard-resources update dlp-object on page 2909](#)
- [diagnose fortiguard-resources update fortiap-end-of-support on page 2909](#)
- [diagnose fortiguard-resources update fortixtender-end-of-support on page 2910](#)
- [diagnose fortiguard-resources update fortigate-end-of-support on page 2910](#)
- [diagnose fortiguard-resources update fortiswitch-end-of-support on page 2910](#)
- [diagnose fortiguard-resources update ips-information on page 2910](#)
- [diagnose fortiguard-resources update prefix-links on page 2910](#)
- [diagnose fortiguard-resources update sprite-casb on page 2911](#)
- [diagnose fortiguard-resources update sprite-isdb on page 2911](#)
- [diagnose fortiguard-resources update sprite-map on page 2911](#)
- [diagnose fortiguard-resources update static-links on page 2911](#)
- [diagnose fortiguard-resources update wf-categories on page 2911](#)

diagnose fortiguard-resources delete

Deletes all downloaded files for a FortiGuard resource, restores the original copy if available.

```
diagnose fortiguard-resources delete
```

diagnose fortiguard-resources delete app-categories

Application categories.

```
diagnose fortiguard-resources delete app-categories
```

diagnose fortiguard-resources delete app-info

Application info for a given ID. If no ID given, deletes all application info resources.

```
diagnose fortiguard-resources delete app-info <id>
```

Parameter	Description	Type	Size
<id>	ID of application to be deleted.	string	

diagnose fortiguard-resources delete dlp-object

DLP object info for a given ID. If no ID given, deletes all DLP object info resources.

```
diagnose fortiguard-resources delete dlp-object <id>
```

Parameter	Description	Type	Size
<id>	ID of DLP object to be deleted.	string	

diagnose fortiguard-resources delete fortiap-end-of-support

FortiAP product life cycle information.

```
diagnose fortiguard-resources delete fortiap-end-of-support
```

diagnose fortiguard-resources delete fortiextender-end-of-support

FortiExtender product life cycle information.

```
diagnose fortiguard-resources delete fortiextender-end-of-support
```

diagnose fortiguard-resources delete fortigate-end-of-support

FortiGate product life cycle information.

```
diagnose fortiguard-resources delete fortigate-end-of-support
```

diagnose fortiguard-resources delete fortiswitch-end-of-support

FortiSwitch product life cycle information.

```
diagnose fortiguard-resources delete fortiswitch-end-of-support
```

diagnose fortiguard-resources delete ips-information

IPS information for a given ID. If no ID given, deletes all IPS info resources.

```
diagnose fortiguard-resources delete ips-information <id>
```

Parameter	Description	Type	Size
<id>	ID of IPS to be deleted.	string	

diagnose fortiguard-resources delete prefix-links

Prefix links.

```
diagnose fortiguard-resources delete prefix-links
```

diagnose fortiguard-resources delete sprite-casb

Application icon sprite CASB (CSS & PNG).

```
diagnose fortiguard-resources delete sprite-casb
```

diagnose fortiguard-resources delete sprite-isdb

Application icon sprite ISDB (CSS & PNG).

```
diagnose fortiguard-resources delete sprite-isdb
```

diagnose fortiguard-resources delete sprite-map

Application icon sprite map (CSS & PNG).

```
diagnose fortiguard-resources delete sprite-map
```

diagnose fortiguard-resources delete static-links

Static links.

```
diagnose fortiguard-resources delete static-links
```

diagnose fortiguard-resources delete wf-categories

Web filter categories.

```
diagnose fortiguard-resources delete wf-categories
```

diagnose fortiguard-resources delete-all

Deletes all downloaded FortiGuard resource files (debug image only).

```
diagnose fortiguard-resources delete-all
```

diagnose fortiguard-resources downloads

Settings for download of FortiGuard resources.

```
diagnose fortiguard-resources downloads
```

diagnose fortiguard-resources downloads disable

Disable GUI downloading of resources from FortiGuard.

```
diagnose fortiguard-resources downloads disable
```

diagnose fortiguard-resources downloads enable

Enable GUI downloading of resources from FortiGuard.

```
diagnose fortiguard-resources downloads enable
```

diagnose fortiguard-resources info

View file information of a downloaded FortiGuard resource.

```
diagnose fortiguard-resources info
```

diagnose fortiguard-resources info app-categories

Application categories.

```
diagnose fortiguard-resources info app-categories
```

diagnose fortiguard-resources info app-info

Application info for a given ID.

```
diagnose fortiguard-resources info app-info <id>
```

Parameter	Description	Type	Size
<id>	ID of application to be retrieved.	string	

diagnose fortiguard-resources info dlp-object

DLP object info for a given ID.

```
diagnose fortiguard-resources info dlp-object <id>
```

Parameter	Description	Type	Size
<id>	ID of DLP object to be retrieved.	string	

diagnose fortiguard-resources info fortiap-end-of-support

FortiAP product life cycle information.

```
diagnose fortiguard-resources info fortiap-end-of-support
```

diagnose fortiguard-resources info fortiextender-end-of-support

FortiExtender product life cycle information.

```
diagnose fortiguard-resources info fortiextender-end-of-support
```

diagnose fortiguard-resources info fortigate-end-of-support

FortiGate product life cycle information.

```
diagnose fortiguard-resources info fortigate-end-of-support
```

diagnose fortiguard-resources info fortiswitch-end-of-support

FortiSwitch product life cycle information.

```
diagnose fortiguard-resources info fortiswitch-end-of-support
```

diagnose fortiguard-resources info ips-information

IPS information for a given ID.

```
diagnose fortiguard-resources info ips-information <id>
```

Parameter	Description	Type	Size
<id>	ID of IPS to be retrieved.	string	

diagnose fortiguard-resources info prefix-links

Prefix links.

```
diagnose fortiguard-resources info prefix-links
```


diagnose fortiguard-resources info sprite-casb.css

Application icon sprite CASB (CSS).

```
diagnose fortiguard-resources info sprite-casb.css
```

diagnose fortiguard-resources info sprite-casb.png

Application icon sprite CASB (PNG).

```
diagnose fortiguard-resources info sprite-casb.png
```

diagnose fortiguard-resources info sprite-isdb.css

Application icon sprite ISDB (CSS).

```
diagnose fortiguard-resources info sprite-isdb.css
```

diagnose fortiguard-resources info sprite-isdb.png

Application icon sprite ISDB (PNG).

```
diagnose fortiguard-resources info sprite-isdb.png
```

diagnose fortiguard-resources info sprite-map.css

Application icon sprite map (CSS).

```
diagnose fortiguard-resources info sprite-map.css
```

diagnose fortiguard-resources info sprite-map.png

Application icon sprite map (PNG).

```
diagnose fortiguard-resources info sprite-map.png
```

diagnose fortiguard-resources info static-links

Static links.

```
diagnose fortiguard-resources info static-links
```

diagnose fortiguard-resources info wf-categories

Web filter categories.

```
diagnose fortiguard-resources info wf-categories
```

diagnose fortiguard-resources log

Shows logs for FortiGuard resource prefetch.

```
diagnose fortiguard-resources log
```

diagnose fortiguard-resources log all

All FortiGuard resources.

```
diagnose fortiguard-resources log all
```

diagnose fortiguard-resources log app-categories

Application categories.

```
diagnose fortiguard-resources log app-categories
```

diagnose fortiguard-resources log app-info

Application info for a given ID.

```
diagnose fortiguard-resources log app-info
```

diagnose fortiguard-resources log fortiap-end-of-support

FortiAP product life cycle information.

```
diagnose fortiguard-resources log fortiap-end-of-support
```

diagnose fortiguard-resources log fortiextender-end-of-support

FortiExtender product life cycle information.

```
diagnose fortiguard-resources log fortiextender-end-of-support
```

diagnose fortiguard-resources log fortigate-end-of-support

FortiGate product life cycle information.

```
diagnose fortiguard-resources log fortigate-end-of-support
```

diagnose fortiguard-resources log fortiswitch-end-of-support

FortiSwitch product life cycle information.

```
diagnose fortiguard-resources log fortiswitch-end-of-support
```

diagnose fortiguard-resources log ips-information

IPS information for a given ID.

```
diagnose fortiguard-resources log ips-information
```

diagnose fortiguard-resources log maintainer

FortiGuard resource maintainer log.

```
diagnose fortiguard-resources log maintainer
```

diagnose fortiguard-resources log prefix-links

Prefix links.

```
diagnose fortiguard-resources log prefix-links
```

diagnose fortiguard-resources log sprite-casb

Application icon sprite CASB (CSS & PNG).

```
diagnose fortiguard-resources log sprite-casb
```

diagnose fortiguard-resources log sprite-isdb

Application icon sprite ISDB (CSS & PNG).

```
diagnose fortiguard-resources log sprite-isdb
```

diagnose fortiguard-resources log sprite-map

Application icon sprite map (CSS & PNG).

```
diagnose fortiguard-resources log sprite-map
```

diagnose fortiguard-resources log static-links

Static links.

```
diagnose fortiguard-resources log static-links
```

diagnose fortiguard-resources log wf-categories

Web filter categories.

```
diagnose fortiguard-resources log wf-categories
```

diagnose fortiguard-resources update

Deletes cached files and force downloads the FortiGuard resource (ignores GUI enable/disable).

```
diagnose fortiguard-resources update
```

diagnose fortiguard-resources update app-categories

Application categories.

```
diagnose fortiguard-resources update app-categories
```

diagnose fortiguard-resources update app-info

Application info for a given ID.

```
diagnose fortiguard-resources update app-info <id>
```

Parameter	Description	Type	Size
<id>	ID of application to be retrieved.	string	

diagnose fortiguard-resources update dlp-object

DLP object info for a given ID.

```
diagnose fortiguard-resources update dlp-object <id>
```

Parameter	Description	Type	Size
<id>	ID of DLP object to be retrieved.	string	

diagnose fortiguard-resources update fortiap-end-of-support

FortiAP product life cycle information.

```
diagnose fortiguard-resources update fortiap-end-of-support
```

diagnose fortiguard-resources update fortiextender-end-of-support

FortiExtender product life cycle information.

```
diagnose fortiguard-resources update fortiextender-end-of-support
```

diagnose fortiguard-resources update fortigate-end-of-support

FortiGate product life cycle information.

```
diagnose fortiguard-resources update fortigate-end-of-support
```

diagnose fortiguard-resources update fortiswitch-end-of-support

FortiSwitch product life cycle information.

```
diagnose fortiguard-resources update fortiswitch-end-of-support
```

diagnose fortiguard-resources update ips-information

IPS information for a given ID.

```
diagnose fortiguard-resources update ips-information <id>
```

Parameter	Description	Type	Size
<id>	ID of IPS to be retrieved.	string	

diagnose fortiguard-resources update prefix-links

Prefix links.

```
diagnose fortiguard-resources update prefix-links
```

diagnose fortiguard-resources update sprite-casb

Application icon sprite CASB (CSS & PNG).

```
diagnose fortiguard-resources update sprite-casb
```

diagnose fortiguard-resources update sprite-isdb

Application icon sprite ISDB (CSS & PNG).

```
diagnose fortiguard-resources update sprite-isdb
```

diagnose fortiguard-resources update sprite-map

Application icon sprite map (CSS & PNG).

```
diagnose fortiguard-resources update sprite-map
```

diagnose fortiguard-resources update static-links

Static links.

```
diagnose fortiguard-resources update static-links
```

diagnose fortiguard-resources update wf-categories

Web filter categories.

```
diagnose fortiguard-resources update wf-categories
```

diagnose fortimq

fortimq daemon diagnostics

This topic includes the following commands:

- [diagnose fortimq test on page 2912](#)

diagnose fortimq test

Test fortimq ipc and rabbitmq client

```
diagnose fortimq test
```

diagnose fortism

Forti Security Module

This topic includes the following commands:

- [diagnose fortism domain on page 2912](#)
- [diagnose fortism domain list on page 2912](#)

diagnose fortism domain

Daemon Domain and PID.

```
diagnose fortism domain
```

diagnose fortism domain list

List Daemon App-Pid.

```
diagnose fortism domain list <pid>
```

Parameter	Description	Type	Size
<pid>	Application Process ID.	string	

diagnose fortitoken

FortiToken

This topic includes the following commands:

- [diagnose fortitoken debug on page 2913](#)
- [diagnose fortitoken debug disable on page 2913](#)
- [diagnose fortitoken debug enable on page 2913](#)

- [diagnose fortitoken info on page 2913](#)
- [diagnose fortitoken test on page 2913](#)

diagnose fortitoken debug

Debug enable/disable.

```
diagnose fortitoken debug
```

diagnose fortitoken debug disable

Disable debug output.

```
diagnose fortitoken debug disable
```

diagnose fortitoken debug enable

Enable debug output.

```
diagnose fortitoken debug enable
```

diagnose fortitoken info

Show current drift and status for each FortiToken.

```
diagnose fortitoken info <id>
```

Parameter	Description	Type	Size
<id>	FortiToken ID.	string	

diagnose fortitoken test

Test FortiToken with screen setting for drift of internal clock.

```
diagnose fortitoken test <id> <code> <next code> <screen size>
```

Parameter	Description	Type	Size
<id>	FortiToken ID.	string	

Parameter	Description	Type	Size
<code>	FortiToken code.	string	
<next code>	Next FortiToken code.	string	
<screen size>	Screen size for drift of internal clock.	string	

diagnose fortitoken-cloud

FortiToken Cloud Service.

This topic includes the following commands:

- [diagnose fortitoken-cloud clear on page 2914](#)
- [diagnose fortitoken-cloud debug on page 2914](#)
- [diagnose fortitoken-cloud debug disable on page 2915](#)
- [diagnose fortitoken-cloud debug enable on page 2915](#)
- [diagnose fortitoken-cloud debug info on page 2915](#)
- [diagnose fortitoken-cloud delete on page 2915](#)
- [diagnose fortitoken-cloud migrate-ftm on page 2915](#)
- [diagnose fortitoken-cloud server on page 2916](#)
- [diagnose fortitoken-cloud set-http on page 2916](#)
- [diagnose fortitoken-cloud show on page 2916](#)
- [diagnose fortitoken-cloud sync on page 2916](#)
- [diagnose fortitoken-cloud update on page 2917](#)

diagnose fortitoken-cloud clear

Clear server connection settings for diagnostics.

```
diagnose fortitoken-cloud clear
```

diagnose fortitoken-cloud debug

Enable/disable debug output.

```
diagnose fortitoken-cloud debug
```

diagnose fortitoken-cloud debug disable

Disable debug output.

```
diagnose fortitoken-cloud debug disable
```

diagnose fortitoken-cloud debug enable

Enable debug output.

```
diagnose fortitoken-cloud debug enable
```

diagnose fortitoken-cloud debug info

Debug status.

```
diagnose fortitoken-cloud debug info
```

diagnose fortitoken-cloud delete

Command to delete a user.

```
diagnose fortitoken-cloud delete <string> <string>
```

Parameter	Description	Type	Size
<string>	User name.	string	
<string>	VDOM name.	string	

diagnose fortitoken-cloud migrate-ftm

Perform FTM license migration.

```
diagnose fortitoken-cloud migrate-ftm <string> <string> <string>
```

Parameter	Description	Type	Size
<string>	Enter command: show, start, abort, add-users, delete-users, ftm2ftc.	string	
<string>	FTM license number.	string	

Parameter	Description	Type	Size
<string>	<return> or VDOM name if add-users delete-users and ftm2ftc.	string	

diagnose fortitoken-cloud server

IP address port number and https.

```
diagnose fortitoken-cloud server <xxx.xxx.xxx.xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	IP address.	string	
<xxx>	Port number <0-65535>.	string	

diagnose fortitoken-cloud set-http

Set HTTP status return code for diagnostics only.

```
diagnose fortitoken-cloud set-http <number>
```

Parameter	Description	Type	Size
<number>	Status code (value < 300 clears the error diagnostics).	string	

diagnose fortitoken-cloud show

Display diagnostics information.

```
diagnose fortitoken-cloud show <string> <string> <string>
```

Parameter	Description	Type	Size
<string>	Enter <server service users user>.	string	
<string>	Enter username to get user information otherwise enter return.	string	
<string>	Enter VDOM name if getting user information.	string	

diagnose fortitoken-cloud sync

Synchronize user information with FortiToken Cloud.

```
diagnose fortitoken-cloud sync <user type>
```

Parameter	Description	Type	Size
<user type>	Enter <return>, all, local, or remote.	string	

diagnose fortitoken-cloud update

Update cache data manually.

```
diagnose fortitoken-cloud update <string> <number>
```

Parameter	Description	Type	Size
<string>	Enter <balance count>.	string	
<number>	argument.	string	

diagnose fortiview

Fortiview backend diagnostic

This topic includes the following commands:

- [diagnose fortiview device on page 2917](#)
- [diagnose fortiview result on page 2917](#)
- [diagnose fortiview sortby on page 2918](#)
- [diagnose fortiview time on page 2918](#)
- [diagnose fortiview view on page 2918](#)

diagnose fortiview device

device

```
diagnose fortiview device
```

diagnose fortiview result

result

```
diagnose fortiview result
```

diagnose fortiview sortby

sortby

```
diagnose fortiview sortby
```

diagnose fortiview time

time

```
diagnose fortiview time
```

diagnose fortiview view

view

```
diagnose fortiview view
```

diagnose geoip

Diagnose geography IP database and service.

This topic includes the following commands:

- [diagnose geoip delete-geoip-db on page 2918](#)
- [diagnose geoip geoip-query on page 2918](#)
- [diagnose geoip ip2country on page 2919](#)
- [diagnose geoip iprange on page 2919](#)
- [diagnose geoip iprange6 on page 2919](#)

diagnose geoip delete-geoip-db

Delete geography IP database currently saved on this FortiGate unit.

```
diagnose geoip delete-geoip-db
```

diagnose geoip geoip-query

Query FortiGuard service for geography information based on IP address.

```
diagnose geoip geoip-query <ip>
```

Parameter	Description	Type	Size
<ip>	IPv4 address.	string	

diagnose geoip ip2country

Query local geography IP database for country information based on IP address.

```
diagnose geoip ip2country <ip>
```

Parameter	Description	Type	Size
<ip>	IPv4/IPv6 address.	string	

diagnose geoip iprange

List IP ranges of specified country.

```
diagnose geoip iprange
```

diagnose geoip iprange6

List IPv6 ranges of specified country.

```
diagnose geoip iprange6
```

diagnose hardware

hardware

This topic includes the following commands:

- [diagnose hardware certificate on page 2920](#)
- [diagnose hardware deviceinfo on page 2920](#)
- [diagnose hardware deviceinfo disk on page 2920](#)
- [diagnose hardware deviceinfo nic on page 2920](#)
- [diagnose hardware deviceinfo nic-channel on page 2921](#)
- [diagnose hardware deviceinfo nic-stats on page 2921](#)
- [diagnose hardware getcbp on page 2921](#)

- [diagnose hardware ioport on page 2921](#)
- [diagnose hardware ioport byte on page 2921](#)
- [diagnose hardware ioport long on page 2921](#)
- [diagnose hardware ioport word on page 2922](#)
- [diagnose hardware lspci on page 2922](#)
- [diagnose hardware mii on page 2922](#)
- [diagnose hardware setcbp on page 2922](#)
- [diagnose hardware setpci on page 2922](#)
- [diagnose hardware sysinfo on page 2922](#)
- [diagnose hardware sysinfo conserve on page 2923](#)
- [diagnose hardware sysinfo cpu on page 2923](#)
- [diagnose hardware sysinfo interrupts on page 2923](#)
- [diagnose hardware sysinfo iomem on page 2923](#)
- [diagnose hardware sysinfo ioports on page 2923](#)
- [diagnose hardware sysinfo memory on page 2923](#)
- [diagnose hardware sysinfo mtrr on page 2924](#)
- [diagnose hardware sysinfo slab on page 2924](#)

diagnose hardware certificate

Verify certificates.

```
diagnose hardware certificate
```

diagnose hardware deviceinfo

Get device information.

```
diagnose hardware deviceinfo
```

diagnose hardware deviceinfo disk

Display information of all disks.

```
diagnose hardware deviceinfo disk
```

diagnose hardware deviceinfo nic

Display NIC information.


```
diagnose hardware deviceinfo nic
```

diagnose hardware deviceinfo nic-channel

Display NIC channels.

```
diagnose hardware deviceinfo nic-channel
```

diagnose hardware deviceinfo nic-stats

Display NIC statistics.

```
diagnose hardware deviceinfo nic-stats
```

diagnose hardware getcbp

Get current CBP mode state.

```
diagnose hardware getcbp
```

diagnose hardware ioport

Read/write data via IO port.

```
diagnose hardware ioport
```

diagnose hardware ioport byte

Read/write byte via IO port.

```
diagnose hardware ioport byte
```

diagnose hardware ioport long

Read/write long via IO port.

```
diagnose hardware ioport long
```

diagnose hardware ioport word

Read/write word via IO port.

```
diagnose hardware ioport word
```

diagnose hardware lspci

List PCI parameters.

```
diagnose hardware lspci
```

diagnose hardware mii

Access mii registers.

```
diagnose hardware mii
```

diagnose hardware setcbp

Set CBP mode before CBP tests.

```
diagnose hardware setcbp
```

diagnose hardware setpci

Set PCI parameters.

```
diagnose hardware setpci
```

diagnose hardware sysinfo

Get system information.

```
diagnose hardware sysinfo
```

diagnose hardware sysinfo conserve

Display information about memory conservation status.

```
diagnose hardware sysinfo conserve
```

diagnose hardware sysinfo cpu

Display detailed information for all installed CPU(s).

```
diagnose hardware sysinfo cpu
```

diagnose hardware sysinfo interrupts

Display system interrupts information.

```
diagnose hardware sysinfo interrupts
```

diagnose hardware sysinfo iomem

Display memory map of I/O ports.

```
diagnose hardware sysinfo iomem
```

diagnose hardware sysinfo ioports

Display address list of I/O ports.

```
diagnose hardware sysinfo ioports
```

diagnose hardware sysinfo memory

Display system memory information.

```
diagnose hardware sysinfo memory
```

diagnose hardware sysinfo mtrr

Display memory type range register.

```
diagnose hardware sysinfo mtrr
```

diagnose hardware sysinfo slab

Display memory allocation information.

```
diagnose hardware sysinfo slab
```

diagnose internet-service

Internet Service Database.

This topic includes the following commands:

- [diagnose internet-service id on page 2924](#)
- [diagnose internet-service id-summary on page 2924](#)
- [diagnose internet-service info on page 2925](#)
- [diagnose internet-service match on page 2925](#)
- [diagnose internet-service sld on page 2925](#)
- [diagnose internet-service status-read on page 2926](#)

diagnose internet-service id

Internet Service ID.

```
diagnose internet-service id <id>
```

Parameter	Description	Type	Size
<id>	Internet Service ID(a nonzero integer).	string	

diagnose internet-service id-summary

Internet Service ID summary.

```
diagnose internet-service id-summary <id>
```

Parameter	Description	Type	Size
<id>	Internet Service ID(a nonzero integer)	string	

diagnose internet-service info

VD and 3T information, include vdomname, protocol, port and IP address

```
diagnose internet-service info <vdomname> <proto> <port> <ip> <priority-id-list>
```

Parameter	Description	Type	Size
<vdomname>	VDOM name	string	
<proto>	Service protocol(0-255) for instance: tcp is 6	string	
<port>	Service port(0-65535).	string	
<ip>	Service IP address.	string	
<priority-id-list>	List of Internet Service ID as priority match.	string	

diagnose internet-service match

Find all matched Internet Services for a specific IP address and netmask.

```
diagnose internet-service match <vdomname> <ip> <netmask>
```

Parameter	Description	Type	Size
<vdomname>	VDOM name.	string	
<ip>	IP address.	string	
<netmask>	Netmask (x.x.x.x).	string	

diagnose internet-service sld

Find second level domain for a specific IP address in the ISDB.

```
diagnose internet-service sld <vdomname> <ip>
```

Parameter	Description	Type	Size
<vdomname>	VDOM name.	string	
<ip>	IP address.	string	

diagnose internet-service status-read

read internet service loading status

```
diagnose internet-service status-read
```

diagnose internet-service6

Internet Service Database.

This topic includes the following commands:

- [diagnose internet-service6 id on page 2926](#)
- [diagnose internet-service6 id-summary on page 2926](#)
- [diagnose internet-service6 info on page 2926](#)
- [diagnose internet-service6 match on page 2927](#)

diagnose internet-service6 id

Internet Service ID.

```
diagnose internet-service6 id <id>
```

Parameter	Description	Type	Size
<id>	Internet Service ID(a nonzero integer).	string	

diagnose internet-service6 id-summary

Internet Service ID summary.

```
diagnose internet-service6 id-summary <id>
```

Parameter	Description	Type	Size
<id>	Internet Service ID(a nonzero integer)	string	

diagnose internet-service6 info

VD and 3T information, include vdname, protocol, port and IP address

```
diagnose internet-service6 info <vdname> <proto> <port> <ip> <priority-id-list>
```

Parameter	Description	Type	Size
<vdname>	VDOM name	string	
<proto>	Service protocol(0-255) for instance: tcp is 6	string	
<port>	Service port(0-65535).	string	
<ip>	Service IP address.	string	
<priority-id-list>	List of Internet Service ID as priority match.	string	

diagnose internet-service6 match

Find all matched Internet Services for a specific IP address and prefix.

```
diagnose internet-service6 match <vdname> <ip> <prefix>
```

Parameter	Description	Type	Size
<vdname>	VDOM name.	string	
<ip>	IP address.	string	
<prefix>	prefix(0-128).	string	

diagnose internet-service-name

Internet Service Name diagnose commands.

This topic includes the following commands:

- [diagnose internet-service-name check-duplicate on page 2927](#)
- [diagnose internet-service-name cleanup on page 2928](#)
- [diagnose internet-service-name list on page 2928](#)

diagnose internet-service-name check-duplicate

Check duplicate name for same Internet Service information.

```
diagnose internet-service-name check-duplicate
```

diagnose internet-service-name cleanup

Clean up unused obsolete Internet Service name.

```
diagnose internet-service-name cleanup
```

diagnose internet-service-name list

Search Internet Service name by detailed information.

```
diagnose internet-service-name list <internet-service-id> <country/aread-id> <region-id> <city-id>
```

Parameter	Description	Type	Size
<internet-service-id>	Internet Service ID to be checked.	string	
<country/aread-id>	Country ID of Internet Service location.	string	
<region-id>	Region ID of Internet Service location.	string	
<city-id>	City ID of Internet Service location.	string	

diagnose ip address

IP addresses.

This topic includes the following commands:

- [diagnose ip address add on page 2928](#)
- [diagnose ip address delete on page 2929](#)
- [diagnose ip address list on page 2929](#)

diagnose ip address add

Add IP address.

```
diagnose ip address add <intf-name> <XXX.XXX.XXX.XXX> <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	
<XXX.XXX.XXX.XXX>	IP network mask.	string	

diagnose ip address delete

Delete IP address.

```
diagnose ip address delete <intf-name> <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	

diagnose ip address list

List IP addresses.

```
diagnose ip address list
```

diagnose ip arp

ARP table.

This topic includes the following commands:

- [diagnose ip arp add on page 2929](#)
- [diagnose ip arp delete on page 2930](#)
- [diagnose ip arp list on page 2930](#)

diagnose ip arp add

Add an ARP entry.

```
diagnose ip arp add <intf-name> <XXX.XXX.XXX.XXX> <XX:XX:XX:XX:XX:XX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	
<XX:XX:XX:XX:XX:XX>	MAC address.	string	

diagnose ip arp delete

Delete an ARP entry.

```
diagnose ip arp delete <intf-name> <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	

diagnose ip arp list

Show ARP table.

```
diagnose ip arp list
```

diagnose ip gre-tunnel

tunnels

This topic includes the following commands:

- [diagnose ip gre-tunnel list on page 2930](#)

diagnose ip gre-tunnel list

Show tunnels.

```
diagnose ip gre-tunnel list
```

diagnose ip ipip-tunnel

tunnels

This topic includes the following commands:

- [diagnose ip ipip-tunnel list on page 2931](#)

diagnose ip ipip-tunnel list

Show tunnels.

```
diagnose ip ipip-tunnel list
```

diagnose ip multicast

Multicast information.

This topic includes the following commands:

- [diagnose ip multicast get-igmp-limit on page 2931](#)
- [diagnose ip multicast group-membership on page 2931](#)
- [diagnose ip multicast mac on page 2931](#)
- [diagnose ip multicast mfc-add on page 2932](#)
- [diagnose ip multicast mfc-del on page 2932](#)
- [diagnose ip multicast mfc-flush on page 2932](#)
- [diagnose ip multicast mroute on page 2932](#)
- [diagnose ip multicast status on page 2933](#)
- [diagnose ip multicast vif on page 2933](#)

diagnose ip multicast get-igmp-limit

Get max IGMP states.

```
diagnose ip multicast get-igmp-limit
```

diagnose ip multicast group-membership

Multicast group membership.

```
diagnose ip multicast group-membership
```

diagnose ip multicast mac

Multicast MAC listing.

```
diagnose ip multicast mac
```

diagnose ip multicast mfc-add

add multicast forwarding cache

```
diagnose ip multicast mfc-add <in-port> <src-ip> <group-ip> <out-ports-map> <vrf>
```

Parameter	Description	Type	Size
<in-port>	vif index of ingress	string	
<src-ip>	Source IP.	string	
<group-ip>	multicast group IP	string	
<out-ports-map>	vif index map of egress ports, e.g. 0xff	string	
<vrf>	VRF ID	string	

diagnose ip multicast mfc-del

delete multicast forwarding cache

```
diagnose ip multicast mfc-del <src-ip> <group-ip> <vrf>
```

Parameter	Description	Type	Size
<src-ip>	Source IP.	string	
<group-ip>	multicast group IP	string	
<vrf>	VRF ID	string	

diagnose ip multicast mfc-flush

Flush multicast routes.

```
diagnose ip multicast mfc-flush
```

diagnose ip multicast mroute

Multicast FIB.

```
diagnose ip multicast mroute
```

diagnose ip multicast status

Multicast status.

```
diagnose ip multicast status
```

diagnose ip multicast vif

Multicast VIF device info.

```
diagnose ip multicast vif
```

diagnose ip parp

Proxy-ARP table.

This topic includes the following commands:

- [diagnose ip parp list on page 2933](#)

diagnose ip parp list

Show Proxy-ARP table.

```
diagnose ip parp list
```

diagnose ip proute

Policy routing.

This topic includes the following commands:

- [diagnose ip proute match on page 2933](#)

diagnose ip proute match

Match policy route.

```
diagnose ip proute match <XXX.XXX.XXX.XXX> <address string> <intf-name> <1-255> <0-65535> <0-65535> <0-511>
```

Parameter	Description	Type	Size
<XXX.XXX.XXX.XXX>	Destination IP address.	string	
<address string>	Source IP or MAC address.	string	
<intf-name>	Interface Name.	string	
<1-255>	Protocol.	string	
<0-65535>	Destination port.	string	
<0-65535>	Source port.	string	
<0-511>	VRF.	string	

diagnose ip route

Routing table.

This topic includes the following commands:

- [diagnose ip route add on page 2934](#)
- [diagnose ip route delete on page 2935](#)
- [diagnose ip route list on page 2935](#)
- [diagnose ip route match on page 2935](#)
- [diagnose ip route verify on page 2936](#)

diagnose ip route add

Add static route.

```
diagnose ip route add <intf-name> <XXX.XXX.XXX.XXX> <XXX.XXX.XXX.XXX> <XXX.XXX.XXX.XXX> <1-255> <0-4294967295> <verify> <ha>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	
<XXX.XXX.XXX.XXX>	IP network mask.	string	
<XXX.XXX.XXX.XXX>	Nextthop IP address.	string	
<1-255>	Route distance.	string	

Parameter	Description	Type	Size
<0-4294967295>	Route priority.	string	
<verify>	Verify operation.	string	
<ha>	HA protocol	string	

diagnose ip route delete

Delete static route.

```
diagnose ip route delete <intf-name> <XXX.XXX.XXX.XXX> <XXX.XXX.XXX.XXX> <XXX.XXX.XXX.XXX> <1-255> <0-4294967295> <verify> <ha>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	
<XXX.XXX.XXX.XXX>	IP network mask.	string	
<XXX.XXX.XXX.XXX>	Nexthop IP address.	string	
<1-255>	Route distance.	string	
<0-4294967295>	Route priority.	string	
<verify>	Verify operation.	string	
<ha>	HA protocol	string	

diagnose ip route list

List routing table.

```
diagnose ip route list
```

diagnose ip route match

Match kernel route.

```
diagnose ip route match <XXX.XXX.XXX.XXX> <XXX.XXX.XXX.XXX> <intf-name> <intf-name> <0-511>
```

Parameter	Description	Type	Size
<XXX.XXX.XXX.XXX>	Destination address.	string	

Parameter	Description	Type	Size
<XXX.XXX.XXX.XXX>	Source address.	string	
<intf-name>	Outgoing interface.	string	
<intf-name>	Incoming interface.	string	
<0-511>	VRF.	string	

diagnose ip route verify

Verify static route.

```
diagnose ip route verify <intf-name> <XXX.XXX.XXX.XXX> <XXX.XXX.XXX.XXX> <XXX.XXX.XXX.XXX> <1-255>  
<0-4294967295>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	
<XXX.XXX.XXX.XXX>	IP network mask.	string	
<XXX.XXX.XXX.XXX>	Nexthop IP address.	string	
<1-255>	Route distance.	string	
<0-4294967295>	Route priority.	string	

diagnose ip router bfd

BFD debug.

This topic includes the following commands:

- [diagnose ip router bfd all on page 2937](#)
- [diagnose ip router bfd cmdb on page 2937](#)
- [diagnose ip router bfd events on page 2937](#)
- [diagnose ip router bfd filter on page 2937](#)
- [diagnose ip router bfd fsm on page 2937](#)
- [diagnose ip router bfd nl on page 2937](#)
- [diagnose ip router bfd packet on page 2938](#)
- [diagnose ip router bfd show on page 2938](#)

diagnose ip router bfd all

Enable/disable all debugging.

```
diagnose ip router bfd all
```

diagnose ip router bfd cmdb

Enable/disable BFD CMDDB debug.

```
diagnose ip router bfd cmdb
```

diagnose ip router bfd events

Enable/disable BFD events debug.

```
diagnose ip router bfd events
```

diagnose ip router bfd filter

Destination/neighbor IP to filter debug, or "clear".

```
diagnose ip router bfd filter
```

diagnose ip router bfd fsm

Enable/disable BFD finite state machine debug.

```
diagnose ip router bfd fsm
```

diagnose ip router bfd nl

Enable/disable BFD ZebOS debug.

```
diagnose ip router bfd nl
```

diagnose ip router bfd packet

Enable/disable BFD packets debug.

```
diagnose ip router bfd packet
```

diagnose ip router bfd show

Show status of BFD debug.

```
diagnose ip router bfd show
```

diagnose ip router bgp

BGP protocol.

This topic includes the following commands:

- [diagnose ip router bgp all on page 2938](#)
- [diagnose ip router bgp dampening on page 2939](#)
- [diagnose ip router bgp events on page 2939](#)
- [diagnose ip router bgp filters on page 2939](#)
- [diagnose ip router bgp fsm on page 2939](#)
- [diagnose ip router bgp keepalives on page 2939](#)
- [diagnose ip router bgp level on page 2939](#)
- [diagnose ip router bgp level critical on page 2940](#)
- [diagnose ip router bgp level error on page 2940](#)
- [diagnose ip router bgp level info on page 2940](#)
- [diagnose ip router bgp level none on page 2940](#)
- [diagnose ip router bgp level warn on page 2940](#)
- [diagnose ip router bgp nsm on page 2940](#)
- [diagnose ip router bgp set-filter on page 2941](#)
- [diagnose ip router bgp show on page 2941](#)
- [diagnose ip router bgp updates on page 2941](#)

diagnose ip router bgp all

Enable all debugging.

```
diagnose ip router bgp all
```

diagnose ip router bgp dampening

BGP dampening.

```
diagnose ip router bgp dampening
```

diagnose ip router bgp events

BGP events.

```
diagnose ip router bgp events
```

diagnose ip router bgp filters

BGP filters.

```
diagnose ip router bgp filters
```

diagnose ip router bgp fsm

BGP finite state machine.

```
diagnose ip router bgp fsm
```

diagnose ip router bgp keepalives

BGP keep alive messages.

```
diagnose ip router bgp keepalives
```

diagnose ip router bgp level

Debug level.

```
diagnose ip router bgp level
```

diagnose ip router bgp level critical

Critical level.

```
diagnose ip router bgp level critical
```

diagnose ip router bgp level error

Error level.

```
diagnose ip router bgp level error
```

diagnose ip router bgp level info

Information level.

```
diagnose ip router bgp level info
```

diagnose ip router bgp level none

None level.

```
diagnose ip router bgp level none
```

diagnose ip router bgp level warn

Warning level.

```
diagnose ip router bgp level warn
```

diagnose ip router bgp nsm

BGP NSM information.

```
diagnose ip router bgp nsm
```

diagnose ip router bgp set-filter

Set BGP debug output filter.

```
diagnose ip router bgp set-filter
```

diagnose ip router bgp show

Show status of BGP debugging.

```
diagnose ip router bgp show
```

diagnose ip router bgp updates

BGP updates.

```
diagnose ip router bgp updates
```

diagnose ip router command

Send command to routing daemon.

This topic includes the following commands:

- [diagnose ip router command show on page 2941](#)
- [diagnose ip router command show-vrf on page 2941](#)

diagnose ip router command show

Send show command to imi.

```
diagnose ip router command show
```

diagnose ip router command show-vrf

Send show command to imi (in virtual router).

```
diagnose ip router command show-vrf
```

diagnose ip router igmp

IGMP debug.

This topic includes the following commands:

- [diagnose ip router igmp all on page 2942](#)
- [diagnose ip router igmp decode on page 2942](#)
- [diagnose ip router igmp encode on page 2942](#)
- [diagnose ip router igmp events on page 2943](#)
- [diagnose ip router igmp fsm on page 2943](#)
- [diagnose ip router igmp level on page 2943](#)
- [diagnose ip router igmp level critical on page 2943](#)
- [diagnose ip router igmp level error on page 2943](#)
- [diagnose ip router igmp level info on page 2943](#)
- [diagnose ip router igmp level none on page 2944](#)
- [diagnose ip router igmp level warn on page 2944](#)
- [diagnose ip router igmp show on page 2944](#)
- [diagnose ip router igmp tib on page 2944](#)

diagnose ip router igmp all

All debugging.

```
diagnose ip router igmp all
```

diagnose ip router igmp decode

Decode debugging.

```
diagnose ip router igmp decode
```

diagnose ip router igmp encode

Encode debugging.

```
diagnose ip router igmp encode
```

diagnose ip router igmp events

Events debugging.

```
diagnose ip router igmp events
```

diagnose ip router igmp fsm

FSM debugging.

```
diagnose ip router igmp fsm
```

diagnose ip router igmp level

Debug level.

```
diagnose ip router igmp level
```

diagnose ip router igmp level critical

Critical level.

```
diagnose ip router igmp level critical
```

diagnose ip router igmp level error

Error level.

```
diagnose ip router igmp level error
```

diagnose ip router igmp level info

Information level.

```
diagnose ip router igmp level info
```

diagnose ip router igmp level none

None level.

```
diagnose ip router igmp level none
```

diagnose ip router igmp level warn

Warning level.

```
diagnose ip router igmp level warn
```

diagnose ip router igmp show

Show status of IGMP debugging.

```
diagnose ip router igmp show
```

diagnose ip router igmp tib

TIB (tree-info-base) debugging.

```
diagnose ip router igmp tib
```

diagnose ip router isis

IS-IS protocol.

This topic includes the following commands:

- [diagnose ip router isis all on page 2945](#)
- [diagnose ip router isis events on page 2945](#)
- [diagnose ip router isis ifsm on page 2945](#)
- [diagnose ip router isis level on page 2945](#)
- [diagnose ip router isis level critical on page 2945](#)
- [diagnose ip router isis level error on page 2945](#)
- [diagnose ip router isis level info on page 2946](#)
- [diagnose ip router isis level none on page 2946](#)
- [diagnose ip router isis level warn on page 2946](#)
- [diagnose ip router isis lsp on page 2946](#)

- [diagnose ip router isis nfsm on page 2946](#)
- [diagnose ip router isis nsm on page 2946](#)
- [diagnose ip router isis pdu on page 2947](#)
- [diagnose ip router isis show on page 2947](#)
- [diagnose ip router isis spf on page 2947](#)

diagnose ip router isis all

Enable all debugging.

```
diagnose ip router isis all
```

diagnose ip router isis events

IS-IS Events.

```
diagnose ip router isis events
```

diagnose ip router isis ifsm

IS-IS Interface State Machine.

```
diagnose ip router isis ifsm
```

diagnose ip router isis level

Debug level.

```
diagnose ip router isis level
```

diagnose ip router isis level critical

Critical level.

```
diagnose ip router isis level critical
```

diagnose ip router isis level error

Error level.

```
diagnose ip router isis level error
```

diagnose ip router isis level info

Information level.

```
diagnose ip router isis level info
```

diagnose ip router isis level none

None level.

```
diagnose ip router isis level none
```

diagnose ip router isis level warn

Warning level.

```
diagnose ip router isis level warn
```

diagnose ip router isis lsp

IS-IS Link State PDU.

```
diagnose ip router isis lsp
```

diagnose ip router isis nfsm

IS-IS Neighbor State Machine.

```
diagnose ip router isis nfsm
```

diagnose ip router isis nsm

IS-IS NSM information.

```
diagnose ip router isis nsm
```

diagnose ip router isis pdu

IS-IS Protocol Data Unit.

```
diagnose ip router isis pdu
```

diagnose ip router isis show

Show IS-IS debugging.

```
diagnose ip router isis show
```

diagnose ip router isis spf

IS-IS SPF Calculation.

```
diagnose ip router isis spf
```

diagnose ip router ospf

OSPF protocol.

This topic includes the following commands:

- [diagnose ip router ospf all on page 2948](#)
- [diagnose ip router ospf events on page 2948](#)
- [diagnose ip router ospf ifsm on page 2948](#)
- [diagnose ip router ospf level on page 2948](#)
- [diagnose ip router ospf level critical on page 2948](#)
- [diagnose ip router ospf level error on page 2948](#)
- [diagnose ip router ospf level info on page 2949](#)
- [diagnose ip router ospf level none on page 2949](#)
- [diagnose ip router ospf level warn on page 2949](#)
- [diagnose ip router ospf lsa on page 2949](#)
- [diagnose ip router ospf n fsm on page 2949](#)
- [diagnose ip router ospf nsm on page 2949](#)
- [diagnose ip router ospf packet on page 2950](#)
- [diagnose ip router ospf route on page 2950](#)
- [diagnose ip router ospf show on page 2950](#)

diagnose ip router ospf all

Enable all debugging.

```
diagnose ip router ospf all
```

diagnose ip router ospf events

OSPF events.

```
diagnose ip router ospf events
```

diagnose ip router ospf ifsm

OSPF Interface State Machine.

```
diagnose ip router ospf ifsm
```

diagnose ip router ospf level

Debug level.

```
diagnose ip router ospf level
```

diagnose ip router ospf level critical

Critical level.

```
diagnose ip router ospf level critical
```

diagnose ip router ospf level error

Error level.

```
diagnose ip router ospf level error
```

diagnose ip router ospf level info

Information level.

```
diagnose ip router ospf level info
```

diagnose ip router ospf level none

None level.

```
diagnose ip router ospf level none
```

diagnose ip router ospf level warn

Warning level.

```
diagnose ip router ospf level warn
```

diagnose ip router ospf lsa

OSPF Link State Advertisement.

```
diagnose ip router ospf lsa
```

diagnose ip router ospf nfsm

OSPF Neighbor State Machine.

```
diagnose ip router ospf nfsm
```

diagnose ip router ospf nsm

OSPF NSM interface.

```
diagnose ip router ospf nsm
```

diagnose ip router ospf packet

OSPF Packets.

```
diagnose ip router ospf packet
```

diagnose ip router ospf route

OSPF route information.

```
diagnose ip router ospf route
```

diagnose ip router ospf show

Show status of OSPF debugging.

```
diagnose ip router ospf show
```

diagnose ip router pim-dm

PIM dense-mode.

This topic includes the following commands:

- [diagnose ip router pim-dm all on page 2951](#)
- [diagnose ip router pim-dm context on page 2951](#)
- [diagnose ip router pim-dm decode on page 2951](#)
- [diagnose ip router pim-dm encode on page 2951](#)
- [diagnose ip router pim-dm fsm on page 2951](#)
- [diagnose ip router pim-dm level on page 2951](#)
- [diagnose ip router pim-dm level critical on page 2952](#)
- [diagnose ip router pim-dm level error on page 2952](#)
- [diagnose ip router pim-dm level info on page 2952](#)
- [diagnose ip router pim-dm level none on page 2952](#)
- [diagnose ip router pim-dm level warn on page 2952](#)
- [diagnose ip router pim-dm mrt on page 2952](#)
- [diagnose ip router pim-dm nexthop on page 2953](#)
- [diagnose ip router pim-dm nsm on page 2953](#)
- [diagnose ip router pim-dm show on page 2953](#)
- [diagnose ip router pim-dm vif on page 2953](#)

diagnose ip router pim-dm all

All debugging.

```
diagnose ip router pim-dm all
```

diagnose ip router pim-dm context

VF-VRF context debugging.

```
diagnose ip router pim-dm context
```

diagnose ip router pim-dm decode

Message decode debugging.

```
diagnose ip router pim-dm decode
```

diagnose ip router pim-dm encode

Message encode debugging.

```
diagnose ip router pim-dm encode
```

diagnose ip router pim-dm fsm

FSM debugging.

```
diagnose ip router pim-dm fsm
```

diagnose ip router pim-dm level

Debug level.

```
diagnose ip router pim-dm level
```

diagnose ip router pim-dm level critical

Critical level.

```
diagnose ip router pim-dm level critical
```

diagnose ip router pim-dm level error

Error level.

```
diagnose ip router pim-dm level error
```

diagnose ip router pim-dm level info

Information level.

```
diagnose ip router pim-dm level info
```

diagnose ip router pim-dm level none

None level.

```
diagnose ip router pim-dm level none
```

diagnose ip router pim-dm level warn

Warning level.

```
diagnose ip router pim-dm level warn
```

diagnose ip router pim-dm mrt

Multicast-route-table debugging.

```
diagnose ip router pim-dm mrt
```


diagnose ip router pim-dm nexthop

Nexthop debugging.

```
diagnose ip router pim-dm nexthop
```

diagnose ip router pim-dm nsm

NSM interaction debugging.

```
diagnose ip router pim-dm nsm
```

diagnose ip router pim-dm show

Show status of PIM dense-mode debugging.

```
diagnose ip router pim-dm show
```

diagnose ip router pim-dm vif

Multicast VI debugging.

```
diagnose ip router pim-dm vif
```

diagnose ip router pim-sm

PIM sparse-mode.

This topic includes the following commands:

- [diagnose ip router pim-sm all on page 2954](#)
- [diagnose ip router pim-sm events on page 2955](#)
- [diagnose ip router pim-sm level on page 2955](#)
- [diagnose ip router pim-sm level critical on page 2955](#)
- [diagnose ip router pim-sm level error on page 2955](#)
- [diagnose ip router pim-sm level info on page 2955](#)
- [diagnose ip router pim-sm level none on page 2955](#)
- [diagnose ip router pim-sm level warn on page 2956](#)
- [diagnose ip router pim-sm mfc on page 2956](#)
- [diagnose ip router pim-sm mib on page 2956](#)

- [diagnose ip router pim-sm nexthop on page 2956](#)
- [diagnose ip router pim-sm nsm on page 2956](#)
- [diagnose ip router pim-sm packet on page 2956](#)
- [diagnose ip router pim-sm packet all on page 2957](#)
- [diagnose ip router pim-sm packet in on page 2957](#)
- [diagnose ip router pim-sm packet out on page 2957](#)
- [diagnose ip router pim-sm show on page 2957](#)
- [diagnose ip router pim-sm state on page 2957](#)
- [diagnose ip router pim-sm timer on page 2957](#)
- [diagnose ip router pim-sm timer all on page 2958](#)
- [diagnose ip router pim-sm timer assert on page 2958](#)
- [diagnose ip router pim-sm timer assert all on page 2958](#)
- [diagnose ip router pim-sm timer assert at on page 2958](#)
- [diagnose ip router pim-sm timer bsr on page 2958](#)
- [diagnose ip router pim-sm timer bsr all on page 2958](#)
- [diagnose ip router pim-sm timer bsr bst on page 2959](#)
- [diagnose ip router pim-sm timer bsr crp on page 2959](#)
- [diagnose ip router pim-sm timer hello on page 2959](#)
- [diagnose ip router pim-sm timer hello all on page 2959](#)
- [diagnose ip router pim-sm timer hello ht on page 2959](#)
- [diagnose ip router pim-sm timer hello nlt on page 2959](#)
- [diagnose ip router pim-sm timer hello tht on page 2960](#)
- [diagnose ip router pim-sm timer joinprune on page 2960](#)
- [diagnose ip router pim-sm timer joinprune all on page 2960](#)
- [diagnose ip router pim-sm timer joinprune et on page 2960](#)
- [diagnose ip router pim-sm timer joinprune jt on page 2960](#)
- [diagnose ip router pim-sm timer joinprune kat on page 2960](#)
- [diagnose ip router pim-sm timer joinprune ot on page 2961](#)
- [diagnose ip router pim-sm timer joinprune ppt on page 2961](#)
- [diagnose ip router pim-sm timer register on page 2961](#)
- [diagnose ip router pim-sm timer register all on page 2961](#)
- [diagnose ip router pim-sm timer register rst on page 2961](#)

diagnose ip router pim-sm all

All debugging.

```
diagnose ip router pim-sm all
```

diagnose ip router pim-sm events

Events debugging.

```
diagnose ip router pim-sm events
```

diagnose ip router pim-sm level

Debug level.

```
diagnose ip router pim-sm level
```

diagnose ip router pim-sm level critical

Critical level.

```
diagnose ip router pim-sm level critical
```

diagnose ip router pim-sm level error

Error level.

```
diagnose ip router pim-sm level error
```

diagnose ip router pim-sm level info

Information level.

```
diagnose ip router pim-sm level info
```

diagnose ip router pim-sm level none

None level.

```
diagnose ip router pim-sm level none
```

diagnose ip router pim-sm level warn

Warning level.

```
diagnose ip router pim-sm level warn
```

diagnose ip router pim-sm mfc

MFC debugging.

```
diagnose ip router pim-sm mfc
```

diagnose ip router pim-sm mib

MIB debugging.

```
diagnose ip router pim-sm mib
```

diagnose ip router pim-sm nexthop

Nexthop debugging.

```
diagnose ip router pim-sm nexthop
```

diagnose ip router pim-sm nsm

NSM debugging.

```
diagnose ip router pim-sm nsm
```

diagnose ip router pim-sm packet

Packet debugging.

```
diagnose ip router pim-sm packet
```

diagnose ip router pim-sm packet all

All packet debugging.

```
diagnose ip router pim-sm packet all
```

diagnose ip router pim-sm packet in

Incoming packet debugging.

```
diagnose ip router pim-sm packet in
```

diagnose ip router pim-sm packet out

Outgoing packet debugging.

```
diagnose ip router pim-sm packet out
```

diagnose ip router pim-sm show

Show status of PIM sparse-mode debugging.

```
diagnose ip router pim-sm show
```

diagnose ip router pim-sm state

State debugging.

```
diagnose ip router pim-sm state
```

diagnose ip router pim-sm timer

Timer debugging.

```
diagnose ip router pim-sm timer
```

diagnose ip router pim-sm timer all

All timer debugging.

```
diagnose ip router pim-sm timer all
```

diagnose ip router pim-sm timer assert

Assert timer debugging.

```
diagnose ip router pim-sm timer assert
```

diagnose ip router pim-sm timer assert all

All assert timers.

```
diagnose ip router pim-sm timer assert all
```

diagnose ip router pim-sm timer assert at

Assert timer.

```
diagnose ip router pim-sm timer assert at
```

diagnose ip router pim-sm timer bsr

BSR timer debugging.

```
diagnose ip router pim-sm timer bsr
```

diagnose ip router pim-sm timer bsr all

All BSR timers.

```
diagnose ip router pim-sm timer bsr all
```

diagnose ip router pim-sm timer bsr bst

Bootstrap timer.

```
diagnose ip router pim-sm timer bsr bst
```

diagnose ip router pim-sm timer bsr crp

Candidate-RP timer.

```
diagnose ip router pim-sm timer bsr crp
```

diagnose ip router pim-sm timer hello

Hello timer debugging.

```
diagnose ip router pim-sm timer hello
```

diagnose ip router pim-sm timer hello all

All hello-related timers.

```
diagnose ip router pim-sm timer hello all
```

diagnose ip router pim-sm timer hello ht

Hello timer.

```
diagnose ip router pim-sm timer hello ht
```

diagnose ip router pim-sm timer hello nlt

Neighbor liveliness timer.

```
diagnose ip router pim-sm timer hello nlt
```

diagnose ip router pim-sm timer hello tht

Triggered hello timer.

```
diagnose ip router pim-sm timer hello tht
```

diagnose ip router pim-sm timer joinprune

Join prune timer debugging.

```
diagnose ip router pim-sm timer joinprune
```

diagnose ip router pim-sm timer joinprune all

All join prune timers.

```
diagnose ip router pim-sm timer joinprune all
```

diagnose ip router pim-sm timer joinprune et

Expiry timer.

```
diagnose ip router pim-sm timer joinprune et
```

diagnose ip router pim-sm timer joinprune jt

Join prune timer.

```
diagnose ip router pim-sm timer joinprune jt
```

diagnose ip router pim-sm timer joinprune kat

Keep alive timer.

```
diagnose ip router pim-sm timer joinprune kat
```


diagnose ip router pim-sm timer joinprune ot

Override timer.

```
diagnose ip router pim-sm timer joinprune ot
```

diagnose ip router pim-sm timer joinprune ppt

Prune pending timer.

```
diagnose ip router pim-sm timer joinprune ppt
```

diagnose ip router pim-sm timer register

Register timer debugging.

```
diagnose ip router pim-sm timer register
```

diagnose ip router pim-sm timer register all

All register timers.

```
diagnose ip router pim-sm timer register all
```

diagnose ip router pim-sm timer register rst

Register stop timer.

```
diagnose ip router pim-sm timer register rst
```

diagnose ip router rip

RIP protocol.

This topic includes the following commands:

- [diagnose ip router rip all on page 2962](#)
- [diagnose ip router rip events on page 2962](#)
- [diagnose ip router rip level on page 2962](#)

- [diagnose ip router rip level critical on page 2962](#)
- [diagnose ip router rip level error on page 2962](#)
- [diagnose ip router rip level info on page 2963](#)
- [diagnose ip router rip level none on page 2963](#)
- [diagnose ip router rip level warn on page 2963](#)
- [diagnose ip router rip nsm on page 2963](#)
- [diagnose ip router rip packet on page 2963](#)
- [diagnose ip router rip show on page 2963](#)

diagnose ip router rip all

Enable all debugging.

```
diagnose ip router rip all
```

diagnose ip router rip events

RIP events.

```
diagnose ip router rip events
```

diagnose ip router rip level

Debug level.

```
diagnose ip router rip level
```

diagnose ip router rip level critical

Critical level.

```
diagnose ip router rip level critical
```

diagnose ip router rip level error

Error level.

```
diagnose ip router rip level error
```

diagnose ip router rip level info

Information level.

```
diagnose ip router rip level info
```

diagnose ip router rip level none

None level.

```
diagnose ip router rip level none
```

diagnose ip router rip level warn

Warning level.

```
diagnose ip router rip level warn
```

diagnose ip router rip nsm

RIP NSM interface

```
diagnose ip router rip nsm
```

diagnose ip router rip packet

RIP packets

```
diagnose ip router rip packet
```

diagnose ip router rip show

Show status of RIP debugging.

```
diagnose ip router rip show
```

diagnose ip router zl

Set flag to make diag ip router commands persist after router restart.

This topic includes the following commands:

- [diagnose ip router zl disable on page 2964](#)
- [diagnose ip router zl enable on page 2964](#)
- [diagnose ip router zl show on page 2964](#)

diagnose ip router zl disable

Debug events/level will reset to default after restart.

```
diagnose ip router zl disable
```

diagnose ip router zl enable

Newly enabled debug events/level will persist after router restart.

```
diagnose ip router zl enable
```

diagnose ip router zl show

Show whether flag is set.

```
diagnose ip router zl show
```

diagnose ip rtcache

Routing cache.

This topic includes the following commands:

- [diagnose ip rtcache stats on page 2964](#)

diagnose ip rtcache stats

Get routing cache statistics.

```
diagnose ip rtcache stats
```

diagnose ip tcp

TCP sockets.

This topic includes the following commands:

- [diagnose ip tcp list on page 2965](#)

diagnose ip tcp list

List TCP sockets.

```
diagnose ip tcp list
```

diagnose ip udp

UDP sockets.

This topic includes the following commands:

- [diagnose ip udp list on page 2965](#)

diagnose ip udp list

List UDP sockets.

```
diagnose ip udp list
```

diagnose ips anomaly

IPS anomaly.

This topic includes the following commands:

- [diagnose ips anomaly clear on page 2966](#)
- [diagnose ips anomaly config on page 2966](#)
- [diagnose ips anomaly filter on page 2966](#)

- [diagnose ips anomaly filter clear on page 2966](#)
- [diagnose ips anomaly filter freq on page 2966](#)
- [diagnose ips anomaly filter id on page 2967](#)
- [diagnose ips anomaly filter ip on page 2967](#)
- [diagnose ips anomaly filter pps on page 2967](#)
- [diagnose ips anomaly list on page 2967](#)
- [diagnose ips anomaly status on page 2968](#)

diagnose ips anomaly clear

Clear anomaly meters.

```
diagnose ips anomaly clear
```

diagnose ips anomaly config

List DoS-sensor.

```
diagnose ips anomaly config
```

diagnose ips anomaly filter

List anomaly with filters.

```
diagnose ips anomaly filter
```

diagnose ips anomaly filter clear

Clear anomaly filter.

```
diagnose ips anomaly filter clear
```

diagnose ips anomaly filter freq

frequency

```
diagnose ips anomaly filter freq <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	Frequency from.	string	
<xx>	Frequency to.	string	

diagnose ips anomaly filter id

Anomaly ID.

```
diagnose ips anomaly filter id <xx>
```

Parameter	Description	Type	Size
<xx>	<0-11>	string	

diagnose ips anomaly filter ip

IP and subnet mask.

```
diagnose ips anomaly filter ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	ip	string	
<xxx.xxx.xxx.xxx>	mask	string	

diagnose ips anomaly filter pps

pps

```
diagnose ips anomaly filter pps <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	PPS from.	string	
<xx>	PPS to.	string	

diagnose ips anomaly list

List anomaly meters.

```
diagnose ips anomaly list
```

diagnose ips anomaly status

List anomaly status.

```
diagnose ips anomaly status
```

diagnose ips anomaly6

IPS6 anomaly.

This topic includes the following commands:

- [diagnose ips anomaly6 clear on page 2968](#)
- [diagnose ips anomaly6 config on page 2968](#)
- [diagnose ips anomaly6 filter on page 2968](#)
- [diagnose ips anomaly6 filter clear on page 2969](#)
- [diagnose ips anomaly6 filter freq on page 2969](#)
- [diagnose ips anomaly6 filter id on page 2969](#)
- [diagnose ips anomaly6 filter ip on page 2969](#)
- [diagnose ips anomaly6 filter pps on page 2969](#)
- [diagnose ips anomaly6 list on page 2970](#)
- [diagnose ips anomaly6 status on page 2970](#)

diagnose ips anomaly6 clear

Clear anomaly meters.

```
diagnose ips anomaly6 clear
```

diagnose ips anomaly6 config

List DoS-sensor.

```
diagnose ips anomaly6 config
```

diagnose ips anomaly6 filter

List anomaly with filters.

```
diagnose ips anomaly6 filter
```


diagnose ips anomaly6 filter clear

Clear anomaly filter.

```
diagnose ips anomaly6 filter clear
```

diagnose ips anomaly6 filter freq

frequency

```
diagnose ips anomaly6 filter freq <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	Frequency from.	string	
<xx>	Frequency to.	string	

diagnose ips anomaly6 filter id

Anomaly ID.

```
diagnose ips anomaly6 filter id <xx>
```

Parameter	Description	Type	Size
<xx>	<0-11>	string	

diagnose ips anomaly6 filter ip

IP and subnet mask.

```
diagnose ips anomaly6 filter ip <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>
```

Parameter	Description	Type	Size
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>	ip	string	

diagnose ips anomaly6 filter pps

pps

```
diagnose ips anomaly6 filter pps <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	PPS from.	string	
<xx>	PPS to.	string	

diagnose ips anomaly6 list

List anomaly meters.

```
diagnose ips anomaly6 list
```

diagnose ips anomaly6 status

List anomaly status.

```
diagnose ips anomaly6 status
```

diagnose ips av avengine

Diagnose commands for AV engine.

This topic includes the following commands:

- [diagnose ips av avengine bypass-disable on page 2970](#)
- [diagnose ips av avengine bypass-enable on page 2970](#)
- [diagnose ips av avengine run-diagnose on page 2971](#)

diagnose ips av avengine bypass-disable

Disable AV engine scan bypass.

```
diagnose ips av avengine bypass-disable
```

diagnose ips av avengine bypass-enable

Enable AV engine scan bypass.

```
diagnose ips av avengine bypass-enable
```

diagnose ips av avengine run-diagnose

Run AV engine diagnose commands.

```
diagnose ips av avengine run-diagnose <command>
```

Parameter	Description	Type	Size
<command>	AV engine diagnostic command.	string	

diagnose ips av cache

This topic includes the following commands:

- [diagnose ips av cache clear on page 2971](#)
- [diagnose ips av cache delete on page 2971](#)
- [diagnose ips av cache list on page 2971](#)
- [diagnose ips av cache set-age on page 2972](#)
- [diagnose ips av cache status on page 2972](#)

diagnose ips av cache clear

clear

```
diagnose ips av cache clear
```

diagnose ips av cache delete

delete

```
diagnose ips av cache delete <ID>
```

Parameter	Description	Type	Size
<ID>	<ID>	string	

diagnose ips av cache list

list

```
diagnose ips av cache list
```

diagnose ips av cache set-age

set-age

```
diagnose ips av cache set-age <ID> <age>
```

Parameter	Description	Type	Size
<ID>	<ID>	string	
<age>	<age>	string	

diagnose ips av cache status

status

```
diagnose ips av cache status
```

diagnose ips av mode

Flow-based AV scan mode.

This topic includes the following commands:

- [diagnose ips av mode show on page 2972](#)

Flow-based AV scan mode.

```
diagnose ips av mode hybrid
```

Parameter	Description	Type	Size
hybrid	Enable/disable hybrid scan mode.	option	

diagnose ips av mode show

Show status of hybrid scan mode.

```
diagnose ips av mode show
```

diagnose ips av query

This topic includes the following commands:

- [diagnose ips av query stats on page 2973](#)
- [diagnose ips av query stats-clear on page 2973](#)

diagnose ips av query stats

stats

```
diagnose ips av query stats
```

diagnose ips av query stats-clear

stats-clear

```
diagnose ips av query stats-clear
```

diagnose ips av stats

AntiVirus statistics.

This topic includes the following commands:

- [diagnose ips av stats clear on page 2973](#)
- [diagnose ips av stats show on page 2973](#)

diagnose ips av stats clear

Clear AntiVirus statistics.

```
diagnose ips av stats clear
```

diagnose ips av stats show

Show AntiVirus statistics.

```
diagnose ips av stats show
```

diagnose ips av timeout

Flowav timeout.

This topic includes the following commands:

- [diagnose ips av timeout set on page 2974](#)
- [diagnose ips av timeout show on page 2974](#)

diagnose ips av timeout set

Set av timeout for diagnosis.

```
diagnose ips av timeout set <Integer>
```

Parameter	Description	Type	Size
<Integer>	Timeout range: 5 - 60.	string	

diagnose ips av timeout show

Show current timeout.

```
diagnose ips av timeout show
```

diagnose ips config disable

This topic includes the following commands:

- [diagnose ips config disable log-verbose on page 2974](#)

diagnose ips config disable log-verbose

log-verbose

```
diagnose ips config disable log-verbose
```

diagnose ips config enable

This topic includes the following commands:

- [diagnose ips config enable log-verbose on page 2975](#)

diagnose ips config enable log-verbose

log-verbose

```
diagnose ips config enable log-verbose
```

diagnose ips dac

This topic includes the following commands:

- [diagnose ips dac clear on page 2975](#)
- [diagnose ips dac info on page 2975](#)

diagnose ips dac clear

clear

```
diagnose ips dac clear <age>
```

Parameter	Description	Type	Size
<age>	<age>	string	

diagnose ips dac info

info

```
diagnose ips dac info
```

diagnose ips debug disable

This topic includes the following commands:

- [diagnose ips debug disable all on page 2977](#)
- [diagnose ips debug disable av on page 2977](#)
- [diagnose ips debug disable content on page 2977](#)
- [diagnose ips debug disable content_detail on page 2977](#)
- [diagnose ips debug disable dac on page 2977](#)
- [diagnose ips debug disable detect on page 2977](#)
- [diagnose ips debug disable diameter on page 2978](#)
- [diagnose ips debug disable dissector on page 2978](#)
- [diagnose ips debug disable dns on page 2978](#)
- [diagnose ips debug disable error on page 2978](#)
- [diagnose ips debug disable http on page 2978](#)
- [diagnose ips debug disable im on page 2978](#)
- [diagnose ips debug disable init on page 2979](#)
- [diagnose ips debug disable ipsa on page 2979](#)
- [diagnose ips debug disable log on page 2979](#)
- [diagnose ips debug disable mail on page 2979](#)
- [diagnose ips debug disable mime on page 2979](#)
- [diagnose ips debug disable p2p on page 2979](#)
- [diagnose ips debug disable packet on page 2980](#)
- [diagnose ips debug disable packet_detail on page 2980](#)
- [diagnose ips debug disable packet_dump on page 2980](#)
- [diagnose ips debug disable parse on page 2980](#)
- [diagnose ips debug disable proxy on page 2980](#)
- [diagnose ips debug disable quic on page 2980](#)
- [diagnose ips debug disable rpc on page 2981](#)
- [diagnose ips debug disable sctp on page 2981](#)
- [diagnose ips debug disable session on page 2981](#)
- [diagnose ips debug disable smb on page 2981](#)
- [diagnose ips debug disable ssh on page 2981](#)
- [diagnose ips debug disable ssl on page 2981](#)
- [diagnose ips debug disable state on page 2982](#)
- [diagnose ips debug disable tcp on page 2982](#)
- [diagnose ips debug disable timeout on page 2982](#)
- [diagnose ips debug disable urlfilter on page 2982](#)
- [diagnose ips debug disable voip on page 2982](#)
- [diagnose ips debug disable warn on page 2982](#)

diagnose ips debug disable all

all

```
diagnose ips debug disable all
```

diagnose ips debug disable av

av

```
diagnose ips debug disable av
```

diagnose ips debug disable content

content

```
diagnose ips debug disable content
```

diagnose ips debug disable content_detail

content_detail

```
diagnose ips debug disable content_detail
```

diagnose ips debug disable dac

dac

```
diagnose ips debug disable dac
```

diagnose ips debug disable detect

detect

```
diagnose ips debug disable detect
```

diagnose ips debug disable diameter

diameter

```
diagnose ips debug disable diameter
```

diagnose ips debug disable dissector

dissector

```
diagnose ips debug disable dissector
```

diagnose ips debug disable dns

dns

```
diagnose ips debug disable dns
```

diagnose ips debug disable error

error

```
diagnose ips debug disable error
```

diagnose ips debug disable http

http

```
diagnose ips debug disable http
```

diagnose ips debug disable im

im

```
diagnose ips debug disable im
```

diagnose ips debug disable init

init

```
diagnose ips debug disable init
```

diagnose ips debug disable ipsa

ipsa

```
diagnose ips debug disable ipsa
```

diagnose ips debug disable log

log

```
diagnose ips debug disable log
```

diagnose ips debug disable mail

mail

```
diagnose ips debug disable mail
```

diagnose ips debug disable mime

mime

```
diagnose ips debug disable mime
```

diagnose ips debug disable p2p

p2p

```
diagnose ips debug disable p2p
```

diagnose ips debug disable packet

packet

```
diagnose ips debug disable packet
```

diagnose ips debug disable packet_detail

packet_detail

```
diagnose ips debug disable packet_detail
```

diagnose ips debug disable packet_dump

packet_dump

```
diagnose ips debug disable packet_dump
```

diagnose ips debug disable parse

parse

```
diagnose ips debug disable parse
```

diagnose ips debug disable proxy

proxy

```
diagnose ips debug disable proxy
```

diagnose ips debug disable quic

quic

```
diagnose ips debug disable quic
```

diagnose ips debug disable rpc

rpc

```
diagnose ips debug disable rpc
```

diagnose ips debug disable sctp

sctp

```
diagnose ips debug disable sctp
```

diagnose ips debug disable session

session

```
diagnose ips debug disable session
```

diagnose ips debug disable smb

smb

```
diagnose ips debug disable smb
```

diagnose ips debug disable ssh

ssh

```
diagnose ips debug disable ssh
```

diagnose ips debug disable ssl

ssl

```
diagnose ips debug disable ssl
```

diagnose ips debug disable state

state

```
diagnose ips debug disable state
```

diagnose ips debug disable tcp

tcp

```
diagnose ips debug disable tcp
```

diagnose ips debug disable timeout

timeout

```
diagnose ips debug disable timeout
```

diagnose ips debug disable urlfilter

urlfilter

```
diagnose ips debug disable urlfilter
```

diagnose ips debug disable voip

voip

```
diagnose ips debug disable voip
```

diagnose ips debug disable warn

warn

```
diagnose ips debug disable warn
```

diagnose ips debug enable

This topic includes the following commands:

- [diagnose ips debug enable all on page 2984](#)
- [diagnose ips debug enable av on page 2984](#)
- [diagnose ips debug enable content on page 2984](#)
- [diagnose ips debug enable content_detail on page 2984](#)
- [diagnose ips debug enable dac on page 2984](#)
- [diagnose ips debug enable detect on page 2984](#)
- [diagnose ips debug enable diameter on page 2985](#)
- [diagnose ips debug enable dissector on page 2985](#)
- [diagnose ips debug enable dns on page 2985](#)
- [diagnose ips debug enable error on page 2985](#)
- [diagnose ips debug enable http on page 2985](#)
- [diagnose ips debug enable im on page 2985](#)
- [diagnose ips debug enable init on page 2986](#)
- [diagnose ips debug enable ipsa on page 2986](#)
- [diagnose ips debug enable log on page 2986](#)
- [diagnose ips debug enable mail on page 2986](#)
- [diagnose ips debug enable mime on page 2986](#)
- [diagnose ips debug enable ml on page 2986](#)
- [diagnose ips debug enable p2p on page 2987](#)
- [diagnose ips debug enable packet on page 2987](#)
- [diagnose ips debug enable packet_detail on page 2987](#)
- [diagnose ips debug enable packet_dump on page 2987](#)
- [diagnose ips debug enable parse on page 2987](#)
- [diagnose ips debug enable proxy on page 2987](#)
- [diagnose ips debug enable quic on page 2988](#)
- [diagnose ips debug enable rpc on page 2988](#)
- [diagnose ips debug enable sctp on page 2988](#)
- [diagnose ips debug enable session on page 2988](#)
- [diagnose ips debug enable smb on page 2988](#)
- [diagnose ips debug enable ssh on page 2988](#)
- [diagnose ips debug enable ssl on page 2989](#)
- [diagnose ips debug enable state on page 2989](#)
- [diagnose ips debug enable tcp on page 2989](#)
- [diagnose ips debug enable timeout on page 2989](#)
- [diagnose ips debug enable urlfilter on page 2989](#)
- [diagnose ips debug enable voip on page 2989](#)
- [diagnose ips debug enable warn on page 2990](#)

diagnose ips debug enable all

all

```
diagnose ips debug enable all
```

diagnose ips debug enable av

av

```
diagnose ips debug enable av
```

diagnose ips debug enable content

content

```
diagnose ips debug enable content
```

diagnose ips debug enable content_detail

content_detail

```
diagnose ips debug enable content_detail
```

diagnose ips debug enable dac

dac

```
diagnose ips debug enable dac
```

diagnose ips debug enable detect

detect

```
diagnose ips debug enable detect
```


diagnose ips debug enable diameter

diameter

```
diagnose ips debug enable diameter
```

diagnose ips debug enable dissector

dissector

```
diagnose ips debug enable dissector
```

diagnose ips debug enable dns

dns

```
diagnose ips debug enable dns
```

diagnose ips debug enable error

error

```
diagnose ips debug enable error
```

diagnose ips debug enable http

http

```
diagnose ips debug enable http
```

diagnose ips debug enable im

im

```
diagnose ips debug enable im
```

diagnose ips debug enable init

init

```
diagnose ips debug enable init
```

diagnose ips debug enable ipsa

ipsa

```
diagnose ips debug enable ipsa
```

diagnose ips debug enable log

log

```
diagnose ips debug enable log
```

diagnose ips debug enable mail

mail

```
diagnose ips debug enable mail
```

diagnose ips debug enable mime

mime

```
diagnose ips debug enable mime
```

diagnose ips debug enable ml

ml

```
diagnose ips debug enable ml
```

diagnose ips debug enable p2p

p2p

```
diagnose ips debug enable p2p
```

diagnose ips debug enable packet

packet

```
diagnose ips debug enable packet
```

diagnose ips debug enable packet_detail

packet_detail

```
diagnose ips debug enable packet_detail
```

diagnose ips debug enable packet_dump

packet_dump

```
diagnose ips debug enable packet_dump
```

diagnose ips debug enable parse

parse

```
diagnose ips debug enable parse
```

diagnose ips debug enable proxy

proxy

```
diagnose ips debug enable proxy
```

diagnose ips debug enable quic

quic

```
diagnose ips debug enable quic
```

diagnose ips debug enable rpc

rpc

```
diagnose ips debug enable rpc
```

diagnose ips debug enable sctp

sctp

```
diagnose ips debug enable sctp
```

diagnose ips debug enable session

session

```
diagnose ips debug enable session
```

diagnose ips debug enable smb

smb

```
diagnose ips debug enable smb
```

diagnose ips debug enable ssh

ssh

```
diagnose ips debug enable ssh
```

diagnose ips debug enable ssl

ssl

```
diagnose ips debug enable ssl
```

diagnose ips debug enable state

state

```
diagnose ips debug enable state
```

diagnose ips debug enable tcp

tcp

```
diagnose ips debug enable tcp
```

diagnose ips debug enable timeout

timeout

```
diagnose ips debug enable timeout
```

diagnose ips debug enable urlfilter

urlfilter

```
diagnose ips debug enable urlfilter
```

diagnose ips debug enable voip

voip

```
diagnose ips debug enable voip
```

diagnose ips debug enable warn

warn

```
diagnose ips debug enable warn
```

diagnose ips debug level

This topic includes the following commands:

- [diagnose ips debug level reset on page 2990](#)
- [diagnose ips debug level save on page 2990](#)

diagnose ips debug level reset

reset

```
diagnose ips debug level reset
```

diagnose ips debug level save

save

```
diagnose ips debug level save
```

diagnose ips debug status

This topic includes the following commands:

- [diagnose ips debug status show on page 2990](#)

diagnose ips debug status show

show

```
diagnose ips debug status show
```

diagnose ips debug timelimit

This topic includes the following commands:

- [diagnose ips debug timelimit set on page 2991](#)

diagnose ips debug timelimit set

set

```
diagnose ips debug timelimit set <seconds>
```

Parameter	Description	Type	Size
<seconds>	<seconds>	string	

diagnose ips dissector

This topic includes the following commands:

- [diagnose ips dissector bypass on page 2991](#)
- [diagnose ips dissector dump on page 2991](#)
- [diagnose ips dissector list on page 2992](#)
- [diagnose ips dissector status on page 2992](#)

diagnose ips dissector bypass

bypass

```
diagnose ips dissector bypass <reset | <dissector>> <enable | disable>
```

Parameter	Description	Type	Size
<reset <dissector>>	reset <dissector>	string	
<enable disable>	<enable disable>	string	

diagnose ips dissector dump

dump

```
diagnose ips dissector dump
```

diagnose ips dissector list

list

```
diagnose ips dissector list
```

diagnose ips dissector status

status

```
diagnose ips dissector status
```

diagnose ips filter

This topic includes the following commands:

- [diagnose ips filter clear on page 2992](#)
- [diagnose ips filter process_id on page 2992](#)
- [diagnose ips filter set on page 2993](#)
- [diagnose ips filter status on page 2993](#)
- [diagnose ips filter timelimit on page 2993](#)

diagnose ips filter clear

clear

```
diagnose ips filter clear
```

diagnose ips filter process_id

process_id

```
diagnose ips filter process_id <process id>
```

Parameter	Description	Type	Size
<process id>	<process id>	string	

diagnose ips filter set

set

```
diagnose ips filter set <bpf filter>
```

Parameter	Description	Type	Size
<bpf filter>	bpf filter	string	

diagnose ips filter status

status

```
diagnose ips filter status
```

diagnose ips filter timelimit

timelimit

```
diagnose ips filter timelimit <seconds>
```

Parameter	Description	Type	Size
<seconds>	<seconds>	string	

diagnose ips global rule

Rule file operation.

This topic includes the following commands:

- [diagnose ips global rule reload on page 2993](#)

diagnose ips global rule reload

Reload rule file.

```
diagnose ips global rule reload
```

diagnose ips gtp

This topic includes the following commands:

- [diagnose ips gtp clear on page 2994](#)
- [diagnose ips gtp list on page 2994](#)
- [diagnose ips gtp stats on page 2994](#)
- [diagnose ips gtp stats-clear on page 2995](#)

diagnose ips gtp clear

clear

```
diagnose ips gtp clear [vdom]
```

Parameter	Description	Type	Size
[vdom]	[vdom]	string	

diagnose ips gtp list

list

```
diagnose ips gtp list [vdom]
```

Parameter	Description	Type	Size
[vdom]	[vdom]	string	

diagnose ips gtp stats

stats

```
diagnose ips gtp stats [vdom]
```

Parameter	Description	Type	Size
[vdom]	[vdom]	string	

diagnose ips gtp stats-clear

stats-clear

```
diagnose ips gtp stats-clear
```

diagnose ips ipsa

This topic includes the following commands:

- [diagnose ips ipsa info on page 2995](#)
- [diagnose ips ipsa read-ridmap on page 2995](#)

diagnose ips ipsa info

info

```
diagnose ips ipsa info
```

diagnose ips ipsa read-ridmap

read-ridmap

```
diagnose ips ipsa read-ridmap
```

diagnose ips l2ips

Layer 2 IPS information.

This topic includes the following commands:

- [diagnose ips l2ips stats on page 2995](#)

diagnose ips l2ips stats

Statistics.

```
diagnose ips l2ips stats
```

diagnose ips memory

This topic includes the following commands:

- [diagnose ips memory compact on page 2996](#)
- [diagnose ips memory profiling on page 2996](#)
- [diagnose ips memory status on page 2996](#)
- [diagnose ips memory track on page 2996](#)
- [diagnose ips memory track-glibc on page 2997](#)
- [diagnose ips memory track-print on page 2997](#)
- [diagnose ips memory track-size on page 2997](#)

diagnose ips memory compact

compact

```
diagnose ips memory compact
```

diagnose ips memory profiling

profiling

```
diagnose ips memory profiling <enable/disable/dump>
```

Parameter	Description	Type	Size
<enable/disable/dump>	<enable/disable/dump>	string	

diagnose ips memory status

status

```
diagnose ips memory status
```

diagnose ips memory track

track

```
diagnose ips memory track <enable/disable/clear>
```

Parameter	Description	Type	Size
<enable/disable/clear>	enable/disable/clear	string	

diagnose ips memory track-glibc

track-glibc

```
diagnose ips memory track-glibc <status/enable/disable/dump>
```

Parameter	Description	Type	Size
<status/enable/disable/dump>	<status/enable/disable/dump>	string	

diagnose ips memory track-print

track-print

```
diagnose ips memory track-print <record count>
```

Parameter	Description	Type	Size
<record count>	<record count>	string	

diagnose ips memory track-size

track-size

```
diagnose ips memory track-size <min size> <max size>
```

Parameter	Description	Type	Size
<min size>	<min size>	string	
<max size>	<max size>	string	

diagnose ips packet

This topic includes the following commands:

- [diagnose ips packet clear on page 2998](#)
- [diagnose ips packet status on page 2998](#)

diagnose ips packet clear

clear

```
diagnose ips packet clear
```

diagnose ips packet status

status

```
diagnose ips packet status
```

diagnose ips pme debug

This topic includes the following commands:

- [diagnose ips pme debug disable on page 2998](#)
- [diagnose ips pme debug enable on page 2998](#)
- [diagnose ips pme debug status on page 2999](#)
- [diagnose ips pme debug verbose on page 2999](#)

diagnose ips pme debug disable

disable

```
diagnose ips pme debug disable
```

diagnose ips pme debug enable

enable

```
diagnose ips pme debug enable
```

diagnose ips pme debug status

status

```
diagnose ips pme debug status
```

diagnose ips pme debug verbose

verbose

```
diagnose ips pme debug verbose
```

diagnose ips pme detail

This topic includes the following commands:

- [diagnose ips pme detail addr on page 2999](#)
- [diagnose ips pme detail all on page 2999](#)
- [diagnose ips pme detail auth on page 3000](#)
- [diagnose ips pme detail def_port on page 3000](#)
- [diagnose ips pme detail intf on page 3000](#)
- [diagnose ips pme detail isdb on page 3000](#)
- [diagnose ips pme detail none on page 3000](#)
- [diagnose ips pme detail sched on page 3000](#)
- [diagnose ips pme detail service on page 3001](#)

diagnose ips pme detail addr

addr

```
diagnose ips pme detail addr
```

diagnose ips pme detail all

all

```
diagnose ips pme detail all
```

diagnose ips pme detail auth

auth

```
diagnose ips pme detail auth
```

diagnose ips pme detail def_port

def_port

```
diagnose ips pme detail def_port
```

diagnose ips pme detail intf

intf

```
diagnose ips pme detail intf
```

diagnose ips pme detail isdb

isdb

```
diagnose ips pme detail isdb
```

diagnose ips pme detail none

none

```
diagnose ips pme detail none
```

diagnose ips pme detail sched

sched

```
diagnose ips pme detail sched
```


diagnose ips pme detail service

service

```
diagnose ips pme detail service
```

diagnose ips pme dynamic-address

This topic includes the following commands:

- [diagnose ips pme dynamic-address list on page 3001](#)

diagnose ips pme dynamic-address list

list

```
diagnose ips pme dynamic-address list [vdom]
```

Parameter	Description	Type	Size
[vdom]	[vdom]	string	

diagnose ips pme fabric-address

This topic includes the following commands:

- [diagnose ips pme fabric-address list on page 3001](#)

diagnose ips pme fabric-address list

list

```
diagnose ips pme fabric-address list [vdom]
```

Parameter	Description	Type	Size
[vdom]	[vdom]	string	

diagnose ips pme policy

This topic includes the following commands:

- [diagnose ips pme policy clear-stats](#) on page 3002
- [diagnose ips pme policy def_port](#) on page 3002
- [diagnose ips pme policy list](#) on page 3002
- [diagnose ips pme policy stats](#) on page 3002

diagnose ips pme policy clear-stats

clear-stats

```
diagnose ips pme policy clear-stats [vdom] [polid]
```

Parameter	Description	Type	Size
[vdom]	[vdom]	string	
[polid]	[polid]	string	

diagnose ips pme policy def_port

def_port

```
diagnose ips pme policy def_port
```

diagnose ips pme policy list

list

```
diagnose ips pme policy list
```

diagnose ips pme policy stats

stats

```
diagnose ips pme policy stats
```

diagnose ips raw

Raw socket.

This topic includes the following commands:

- [diagnose ips raw clear on page 3003](#)
- [diagnose ips raw status on page 3003](#)

diagnose ips raw clear

Clear status.

```
diagnose ips raw clear
```

diagnose ips raw status

Show status.

```
diagnose ips raw status
```

diagnose ips session

This topic includes the following commands:

- [diagnose ips session clear on page 3003](#)
- [diagnose ips session content on page 3004](#)
- [diagnose ips session list on page 3004](#)
- [diagnose ips session performance on page 3004](#)
- [diagnose ips session status on page 3004](#)

diagnose ips session clear

clear

```
diagnose ips session clear [vdom]
```

Parameter	Description	Type	Size
[vdom]	[vdom]	string	

diagnose ips session content

content

```
diagnose ips session content
```

diagnose ips session list

list

```
diagnose ips session list <by-mem> <number>
```

Parameter	Description	Type	Size
<by-mem>	by-mem	string	
<number>	<number>	string	

diagnose ips session performance

performance

```
diagnose ips session performance
```

diagnose ips session status

status

```
diagnose ips session status
```

diagnose ips share

This topic includes the following commands:

- [diagnose ips share clear on page 3005](#)
- [diagnose ips share list on page 3005](#)
- [diagnose ips share pool on page 3005](#)

diagnose ips share clear

clear

```
diagnose ips share clear <pool>
```

Parameter	Description	Type	Size
<pool>	<pool>	string	

diagnose ips share list

list

```
diagnose ips share list <pool>
```

Parameter	Description	Type	Size
<pool>	<pool>	string	

diagnose ips share pool

pool

```
diagnose ips share pool
```

diagnose ips shmopts

This topic includes the following commands:

- [diagnose ips shmopts disable on page 3005](#)
- [diagnose ips shmopts list on page 3006](#)
- [diagnose ips shmopts reset on page 3006](#)
- [diagnose ips shmopts status on page 3006](#)

diagnose ips shmopts disable

disable

```
diagnose ips shmopts disable
```

diagnose ips shmopts list

list

```
diagnose ips shmopts list
```

diagnose ips shmopts reset

reset

```
diagnose ips shmopts reset
```

diagnose ips shmopts status

status

```
diagnose ips shmopts status
```

diagnose ips signature

This topic includes the following commands:

- [diagnose ips signature cycle on page 3006](#)
- [diagnose ips signature hit on page 3007](#)
- [diagnose ips signature on-hold on page 3007](#)
- [diagnose ips signature status on page 3007](#)

diagnose ips signature cycle

cycle

```
diagnose ips signature cycle <top N>
```

Parameter	Description	Type	Size
<top N>	<top N>	string	

diagnose ips signature hit

hit

```
diagnose ips signature hit <top N>
```

Parameter	Description	Type	Size
<top N>	<top N>	string	

diagnose ips signature on-hold

on-hold

```
diagnose ips signature on-hold <vdom> <rule id>
```

Parameter	Description	Type	Size
<vdom>	<vdom>	string	
<rule id>	<rule id>	string	

diagnose ips signature status

status

```
diagnose ips signature status <severity mask>
```

Parameter	Description	Type	Size
<severity mask>	<severity mask>	string	

diagnose ips ssl

This topic includes the following commands:

- [diagnose ips ssl bypass on page 3008](#)
- [diagnose ips ssl cc-alg on page 3008](#)
- [diagnose ips ssl ciphers on page 3008](#)
- [diagnose ips ssl clear on page 3008](#)
- [diagnose ips ssl debug on page 3008](#)

- [diagnose ips ssl debug-status on page 3009](#)
- [diagnose ips ssl noscan on page 3009](#)
- [diagnose ips ssl resume on page 3009](#)
- [diagnose ips ssl status on page 3009](#)

diagnose ips ssl bypass

bypass

```
diagnose ips ssl bypass <enable | disable>
```

Parameter	Description	Type	Size
<enable disable>	enable disable	string	

diagnose ips ssl cc-alg

cc-alg

```
diagnose ips ssl cc-alg <bic|cubic>
```

Parameter	Description	Type	Size
<bic cubic>	bic cubic	string	

diagnose ips ssl ciphers

ciphers

```
diagnose ips ssl ciphers
```

diagnose ips ssl clear

clear

```
diagnose ips ssl clear
```

diagnose ips ssl debug

debug


```
diagnose ips ssl debug <none|err|warn|info|dbg|noise>
```

Parameter	Description	Type	Size
<none err warn info dbg noise>	none err warn info dbg noise	string	

diagnose ips ssl debug-status

debug-status

```
diagnose ips ssl debug-status
```

diagnose ips ssl noscan

noscan

```
diagnose ips ssl noscan <enable | disable>
```

Parameter	Description	Type	Size
<enable disable>	enable disable	string	

diagnose ips ssl resume

resume

```
diagnose ips ssl resume <enable | disable>
```

Parameter	Description	Type	Size
<enable disable>	enable disable	string	

diagnose ips ssl status

status

```
diagnose ips ssl status
```

diagnose ips tcp

This topic includes the following commands:

- [diagnose ips tcp clear on page 3010](#)
- [diagnose ips tcp stats on page 3010](#)

diagnose ips tcp clear

clear

```
diagnose ips tcp clear
```

diagnose ips tcp stats

stats

```
diagnose ips tcp stats
```

diagnose ips test

This topic includes the following commands:

- [diagnose ips test cmd on page 3010](#)

diagnose ips test cmd

cmd

```
diagnose ips test cmd <cmd1;cmd2;cmd3>
```

Parameter	Description	Type	Size
<cmd1;cmd2;cmd3>	cmd1;cmd2;cmd3	string	

diagnose ips urlfilter

This topic includes the following commands:

- [diagnose ips urlfilter clear on page 3011](#)
- [diagnose ips urlfilter status on page 3011](#)

diagnose ips urlfilter clear

clear

```
diagnose ips urlfilter clear
```

diagnose ips urlfilter status

status

```
diagnose ips urlfilter status
```

diagnose ips vpatch

This topic includes the following commands:

- [diagnose ips vpatch fmwp-enable-all on page 3011](#)
- [diagnose ips vpatch fmwp-reset on page 3012](#)
- [diagnose ips vpatch fmwp-status on page 3012](#)
- [diagnose ips vpatch ot-status on page 3012](#)
- [diagnose ips vpatch query on page 3012](#)

diagnose ips vpatch fmwp-enable-all

fmwp-enable-all

```
diagnose ips vpatch fmwp-enable-all
```

diagnose ips vpatch fmwp-reset

fmwp-reset

```
diagnose ips vpatch fmwp-reset
```

diagnose ips vpatch fmwp-status

fmwp-status

```
diagnose ips vpatch fmwp-status
```

diagnose ips vpatch ot-status

ot-status

```
diagnose ips vpatch ot-status
```

diagnose ips vpatch query

query

```
diagnose ips vpatch query <device> <MAC>,<IP>
```

Parameter	Description	Type	Size
<device>	<device>	string	
<MAC>,<IP>	<MAC>,<IP>	string	

diagnose ipv6 address

IPv6 addresses.

This topic includes the following commands:

- [diagnose ipv6 address add on page 3013](#)
- [diagnose ipv6 address anycast on page 3013](#)
- [diagnose ipv6 address delete on page 3013](#)
- [diagnose ipv6 address list on page 3013](#)
- [diagnose ipv6 address multicast on page 3013](#)

diagnose ipv6 address add

Add IPv6 address.

```
diagnose ipv6 address add <intf-name> <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>	IPv6 prefix.	string	

diagnose ipv6 address anycast

Add IPv6 anycast address.

```
diagnose ipv6 address anycast
```

diagnose ipv6 address delete

Delete IPv6 address.

```
diagnose ipv6 address delete <intf-name> <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>	IPv6 prefix.	string	

diagnose ipv6 address list

List IPv6 addresses.

```
diagnose ipv6 address list
```

diagnose ipv6 address multicast

Add IPv6 multicast address.

```
diagnose ipv6 address multicast <intf-name> <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>	IPv6 prefix.	string	

diagnose ipv6 devconf

IPv6 device config.

This topic includes the following commands:

- [diagnose ipv6 devconf accept-dad](#) on page 3014
- [diagnose ipv6 devconf disable_ipv6](#) on page 3014

diagnose ipv6 devconf accept-dad

IPv6 Duplicate Address Detection.

```
diagnose ipv6 devconf accept-dad <0, 1 or 2>
```

Parameter	Description	Type	Size
<0, 1 or 2>	0: disable DAD; 1: enable DAD; 2: enable DAD, and disable IPv6 operation if MAC-based duplicate link-local address has been found	string	

diagnose ipv6 devconf disable_ipv6

Disable/enable IPv6 operation.

```
diagnose ipv6 devconf disable_ipv6 <0 or 1>
```

Parameter	Description	Type	Size
<0 or 1>	0: enabling IPv6 operation; 1: disabling.	string	

diagnose ipv6 gre-tunnel

tunnels

This topic includes the following commands:

- [diagnose ipv6 gre-tunnel list on page 3015](#)

diagnose ipv6 gre-tunnel list

Show GRE tunnels.

```
diagnose ipv6 gre-tunnel list
```

diagnose ipv6 ipv6-tunnel

tunnels

This topic includes the following commands:

- [diagnose ipv6 ipv6-tunnel list on page 3015](#)

diagnose ipv6 ipv6-tunnel list

Show tunnels.

```
diagnose ipv6 ipv6-tunnel list
```

diagnose ipv6 multicast

Multicast information.

This topic includes the following commands:

- [diagnose ipv6 multicast mroute on page 3015](#)
- [diagnose ipv6 multicast status on page 3016](#)
- [diagnose ipv6 multicast vif on page 3016](#)

diagnose ipv6 multicast mroute

Multicast FIB.

```
diagnose ipv6 multicast mroute
```

diagnose ipv6 multicast status

Multicast status.

```
diagnose ipv6 multicast status
```

diagnose ipv6 multicast vif

Multicast VIF device info.

```
diagnose ipv6 multicast vif
```

diagnose ipv6 neighbor-cache

IPv6 neighbor-cache table.

This topic includes the following commands:

- [diagnose ipv6 neighbor-cache add on page 3016](#)
- [diagnose ipv6 neighbor-cache delete on page 3016](#)
- [diagnose ipv6 neighbor-cache flush on page 3017](#)
- [diagnose ipv6 neighbor-cache list on page 3017](#)

diagnose ipv6 neighbor-cache add

Add an IPv6 neighbor cache entry.

```
diagnose ipv6 neighbor-cache add <intf-name> <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>  
<XX:XX:XX:XX:XX:XX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>	IPv6 address.	string	
<XX:XX:XX:XX:XX:XX>	MAC address.	string	

diagnose ipv6 neighbor-cache delete

Delete an IPv6 neighbor cache entry.


```
diagnose ipv6 neighbor-cache delete <intf-name> <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>	IPv6 address.	string	

diagnose ipv6 neighbor-cache flush

Flush IPv6 neighbor cache table.

```
diagnose ipv6 neighbor-cache flush <intf-name>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	

diagnose ipv6 neighbor-cache list

Show IPv6 neighbor cache table.

```
diagnose ipv6 neighbor-cache list
```

diagnose ipv6 proute

IPv6 policy routing.

This topic includes the following commands:

- [diagnose ipv6 proute match on page 3017](#)

diagnose ipv6 proute match

Match IPv6 route to policy routes.

```
diagnose ipv6 proute match <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx> <intf-name> <0-255> <0-65535> <0-65535> <0-511>
```

Parameter	Description	Type	Size
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>	IPv6 destination address.	string	

Parameter	Description	Type	Size
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>	Source IP or MAC address.	string	
<intf-name>	Interface Name.	string	
<0-255>	Protocol.	string	
<0-65535>	Destination port.	string	
<0-65535>	Source port.	string	
<0-511>	VRF.	string	

diagnose ipv6 route

IPv6 routing table.

This topic includes the following commands:

- [diagnose ipv6 route list on page 3018](#)

diagnose ipv6 route list

List IPv6 routing table.

```
diagnose ipv6 route list
```

diagnose ipv6 router ospf

OSPFv3 protocol.

This topic includes the following commands:

- [diagnose ipv6 router ospf all on page 3019](#)
- [diagnose ipv6 router ospf events on page 3019](#)
- [diagnose ipv6 router ospf ifsm on page 3019](#)
- [diagnose ipv6 router ospf level on page 3019](#)
- [diagnose ipv6 router ospf level critical on page 3019](#)
- [diagnose ipv6 router ospf level error on page 3019](#)
- [diagnose ipv6 router ospf level info on page 3020](#)
- [diagnose ipv6 router ospf level none on page 3020](#)
- [diagnose ipv6 router ospf level warn on page 3020](#)
- [diagnose ipv6 router ospf lsa on page 3020](#)

- [diagnose ipv6 router ospf nfsm on page 3020](#)
- [diagnose ipv6 router ospf nsm on page 3020](#)
- [diagnose ipv6 router ospf packet on page 3021](#)
- [diagnose ipv6 router ospf route on page 3021](#)
- [diagnose ipv6 router ospf show on page 3021](#)

diagnose ipv6 router ospf all

All OSPFv3 debug.

```
diagnose ipv6 router ospf all
```

diagnose ipv6 router ospf events

OSPFv3 events.

```
diagnose ipv6 router ospf events
```

diagnose ipv6 router ospf ifsm

OSPFv3 Interface State Machine.

```
diagnose ipv6 router ospf ifsm
```

diagnose ipv6 router ospf level

Debug level.

```
diagnose ipv6 router ospf level
```

diagnose ipv6 router ospf level critical

Critical level.

```
diagnose ipv6 router ospf level critical
```

diagnose ipv6 router ospf level error

Error level.

```
diagnose ipv6 router ospf level error
```

diagnose ipv6 router ospf level info

Information level.

```
diagnose ipv6 router ospf level info
```

diagnose ipv6 router ospf level none

None level.

```
diagnose ipv6 router ospf level none
```

diagnose ipv6 router ospf level warn

Warning level.

```
diagnose ipv6 router ospf level warn
```

diagnose ipv6 router ospf lsa

OSPFv3 Link State Advertisement.

```
diagnose ipv6 router ospf lsa
```

diagnose ipv6 router ospf nfsm

OSPFv3 Neighbor State Machine.

```
diagnose ipv6 router ospf nfsm
```

diagnose ipv6 router ospf nsm

OSPFv3 NSM information.

```
diagnose ipv6 router ospf nsm
```

diagnose ipv6 router ospf packet

OSPFv3 packets.

```
diagnose ipv6 router ospf packet
```

diagnose ipv6 router ospf route

OSPFv3 route information.

```
diagnose ipv6 router ospf route
```

diagnose ipv6 router ospf show

Show status of OSPFv3 debugging.

```
diagnose ipv6 router ospf show
```

diagnose ipv6 router pim-sm

PIM sparse-mode.

This topic includes the following commands:

- [diagnose ipv6 router pim-sm all on page 3022](#)
- [diagnose ipv6 router pim-sm events on page 3022](#)
- [diagnose ipv6 router pim-sm level on page 3023](#)
- [diagnose ipv6 router pim-sm level critical on page 3023](#)
- [diagnose ipv6 router pim-sm level error on page 3023](#)
- [diagnose ipv6 router pim-sm level info on page 3023](#)
- [diagnose ipv6 router pim-sm level none on page 3023](#)
- [diagnose ipv6 router pim-sm level warn on page 3023](#)
- [diagnose ipv6 router pim-sm mfc on page 3024](#)
- [diagnose ipv6 router pim-sm mib on page 3024](#)
- [diagnose ipv6 router pim-sm nexthop on page 3024](#)
- [diagnose ipv6 router pim-sm nsm on page 3024](#)
- [diagnose ipv6 router pim-sm packet on page 3024](#)
- [diagnose ipv6 router pim-sm packet all on page 3024](#)
- [diagnose ipv6 router pim-sm packet in on page 3025](#)
- [diagnose ipv6 router pim-sm packet out on page 3025](#)

- [diagnose ipv6 router pim-sm show on page 3025](#)
- [diagnose ipv6 router pim-sm state on page 3025](#)
- [diagnose ipv6 router pim-sm timer on page 3025](#)
- [diagnose ipv6 router pim-sm timer all on page 3025](#)
- [diagnose ipv6 router pim-sm timer assert on page 3026](#)
- [diagnose ipv6 router pim-sm timer assert all on page 3026](#)
- [diagnose ipv6 router pim-sm timer assert at on page 3026](#)
- [diagnose ipv6 router pim-sm timer bsr on page 3026](#)
- [diagnose ipv6 router pim-sm timer bsr all on page 3026](#)
- [diagnose ipv6 router pim-sm timer bsr bst on page 3026](#)
- [diagnose ipv6 router pim-sm timer bsr crp on page 3027](#)
- [diagnose ipv6 router pim-sm timer hello on page 3027](#)
- [diagnose ipv6 router pim-sm timer hello all on page 3027](#)
- [diagnose ipv6 router pim-sm timer hello ht on page 3027](#)
- [diagnose ipv6 router pim-sm timer hello nlt on page 3027](#)
- [diagnose ipv6 router pim-sm timer hello tht on page 3027](#)
- [diagnose ipv6 router pim-sm timer joinprune on page 3028](#)
- [diagnose ipv6 router pim-sm timer joinprune all on page 3028](#)
- [diagnose ipv6 router pim-sm timer joinprune et on page 3028](#)
- [diagnose ipv6 router pim-sm timer joinprune jt on page 3028](#)
- [diagnose ipv6 router pim-sm timer joinprune kat on page 3028](#)
- [diagnose ipv6 router pim-sm timer joinprune ot on page 3028](#)
- [diagnose ipv6 router pim-sm timer joinprune ppt on page 3029](#)
- [diagnose ipv6 router pim-sm timer register on page 3029](#)
- [diagnose ipv6 router pim-sm timer register all on page 3029](#)
- [diagnose ipv6 router pim-sm timer register rst on page 3029](#)

diagnose ipv6 router pim-sm all

All debugging.

```
diagnose ipv6 router pim-sm all
```

diagnose ipv6 router pim-sm events

Events debugging.

```
diagnose ipv6 router pim-sm events
```

diagnose ipv6 router pim-sm level

Debug level.

```
diagnose ipv6 router pim-sm level
```

diagnose ipv6 router pim-sm level critical

Critical level.

```
diagnose ipv6 router pim-sm level critical
```

diagnose ipv6 router pim-sm level error

Error level.

```
diagnose ipv6 router pim-sm level error
```

diagnose ipv6 router pim-sm level info

Information level.

```
diagnose ipv6 router pim-sm level info
```

diagnose ipv6 router pim-sm level none

None level.

```
diagnose ipv6 router pim-sm level none
```

diagnose ipv6 router pim-sm level warn

Warning level.

```
diagnose ipv6 router pim-sm level warn
```

diagnose ipv6 router pim-sm mfc

MFC debugging.

```
diagnose ipv6 router pim-sm mfc
```

diagnose ipv6 router pim-sm mib

MIB debugging.

```
diagnose ipv6 router pim-sm mib
```

diagnose ipv6 router pim-sm nexthop

Nexthop debugging.

```
diagnose ipv6 router pim-sm nexthop
```

diagnose ipv6 router pim-sm nsm

NSM debugging.

```
diagnose ipv6 router pim-sm nsm
```

diagnose ipv6 router pim-sm packet

Packet debugging.

```
diagnose ipv6 router pim-sm packet
```

diagnose ipv6 router pim-sm packet all

All packet debugging.

```
diagnose ipv6 router pim-sm packet all
```


diagnose ipv6 router pim-sm packet in

Incoming packet debugging.

```
diagnose ipv6 router pim-sm packet in
```

diagnose ipv6 router pim-sm packet out

Outgoing packet debugging.

```
diagnose ipv6 router pim-sm packet out
```

diagnose ipv6 router pim-sm show

Show status of PIM sparse-mode debugging.

```
diagnose ipv6 router pim-sm show
```

diagnose ipv6 router pim-sm state

State debugging.

```
diagnose ipv6 router pim-sm state
```

diagnose ipv6 router pim-sm timer

Timer debugging.

```
diagnose ipv6 router pim-sm timer
```

diagnose ipv6 router pim-sm timer all

All timer debugging.

```
diagnose ipv6 router pim-sm timer all
```

diagnose ipv6 router pim-sm timer assert

Assert timer debugging.

```
diagnose ipv6 router pim-sm timer assert
```

diagnose ipv6 router pim-sm timer assert all

All assert timers.

```
diagnose ipv6 router pim-sm timer assert all
```

diagnose ipv6 router pim-sm timer assert at

Assert timer.

```
diagnose ipv6 router pim-sm timer assert at
```

diagnose ipv6 router pim-sm timer bsr

BSR timer debugging.

```
diagnose ipv6 router pim-sm timer bsr
```

diagnose ipv6 router pim-sm timer bsr all

All BSR timers.

```
diagnose ipv6 router pim-sm timer bsr all
```

diagnose ipv6 router pim-sm timer bsr bst

Bootstrap timer.

```
diagnose ipv6 router pim-sm timer bsr bst
```

diagnose ipv6 router pim-sm timer bsr crp

Candidate-RP timer.

```
diagnose ipv6 router pim-sm timer bsr crp
```

diagnose ipv6 router pim-sm timer hello

Hello timer debugging.

```
diagnose ipv6 router pim-sm timer hello
```

diagnose ipv6 router pim-sm timer hello all

All hello-related timers.

```
diagnose ipv6 router pim-sm timer hello all
```

diagnose ipv6 router pim-sm timer hello ht

Hello timer.

```
diagnose ipv6 router pim-sm timer hello ht
```

diagnose ipv6 router pim-sm timer hello nlt

Neighbor liveliness timer.

```
diagnose ipv6 router pim-sm timer hello nlt
```

diagnose ipv6 router pim-sm timer hello tht

Triggered hello timer.

```
diagnose ipv6 router pim-sm timer hello tht
```

diagnose ipv6 router pim-sm timer joinprune

Join prune timer debugging.

```
diagnose ipv6 router pim-sm timer joinprune
```

diagnose ipv6 router pim-sm timer joinprune all

All join prune timers.

```
diagnose ipv6 router pim-sm timer joinprune all
```

diagnose ipv6 router pim-sm timer joinprune et

Expiry timer.

```
diagnose ipv6 router pim-sm timer joinprune et
```

diagnose ipv6 router pim-sm timer joinprune jt

Join prune timer.

```
diagnose ipv6 router pim-sm timer joinprune jt
```

diagnose ipv6 router pim-sm timer joinprune kat

Keep alive timer.

```
diagnose ipv6 router pim-sm timer joinprune kat
```

diagnose ipv6 router pim-sm timer joinprune ot

Override timer.

```
diagnose ipv6 router pim-sm timer joinprune ot
```

diagnose ipv6 router pim-sm timer joinprune ppt

Prune pending timer.

```
diagnose ipv6 router pim-sm timer joinprune ppt
```

diagnose ipv6 router pim-sm timer register

Register timer debugging.

```
diagnose ipv6 router pim-sm timer register
```

diagnose ipv6 router pim-sm timer register all

All register timers.

```
diagnose ipv6 router pim-sm timer register all
```

diagnose ipv6 router pim-sm timer register rst

Register stop timer.

```
diagnose ipv6 router pim-sm timer register rst
```

diagnose ipv6 router rip

RIPng protocol.

This topic includes the following commands:

- [diagnose ipv6 router rip all on page 3030](#)
- [diagnose ipv6 router rip events on page 3030](#)
- [diagnose ipv6 router rip level on page 3030](#)
- [diagnose ipv6 router rip level critical on page 3030](#)
- [diagnose ipv6 router rip level error on page 3030](#)
- [diagnose ipv6 router rip level info on page 3030](#)
- [diagnose ipv6 router rip level none on page 3031](#)
- [diagnose ipv6 router rip level warn on page 3031](#)
- [diagnose ipv6 router rip nsm on page 3031](#)
- [diagnose ipv6 router rip packet on page 3031](#)

- [diagnose ipv6 router rip show on page 3031](#)

diagnose ipv6 router rip all

Enable all debugging.

```
diagnose ipv6 router rip all
```

diagnose ipv6 router rip events

RIPng events.

```
diagnose ipv6 router rip events
```

diagnose ipv6 router rip level

Debug level.

```
diagnose ipv6 router rip level
```

diagnose ipv6 router rip level critical

Critical level.

```
diagnose ipv6 router rip level critical
```

diagnose ipv6 router rip level error

Error level.

```
diagnose ipv6 router rip level error
```

diagnose ipv6 router rip level info

Information level.

```
diagnose ipv6 router rip level info
```

diagnose ipv6 router rip level none

None level.

```
diagnose ipv6 router rip level none
```

diagnose ipv6 router rip level warn

Warning level.

```
diagnose ipv6 router rip level warn
```

diagnose ipv6 router rip nsm

RIPng NSM interface

```
diagnose ipv6 router rip nsm
```

diagnose ipv6 router rip packet

RIPng packets

```
diagnose ipv6 router rip packet
```

diagnose ipv6 router rip show

Show status of RIPng debugging.

```
diagnose ipv6 router rip show
```

diagnose ipv6 router zl6

Set flag to make diag ipv6 router commands persist after router restart.

This topic includes the following commands:

- [diagnose ipv6 router zl6 disable on page 3032](#)
- [diagnose ipv6 router zl6 enable on page 3032](#)
- [diagnose ipv6 router zl6 show on page 3032](#)

diagnose ipv6 router zl6 disable

Debug events/level will reset to default after restart.

```
diagnose ipv6 router zl6 disable
```

diagnose ipv6 router zl6 enable

Newly enabled debug events/level will persist after router restart.

```
diagnose ipv6 router zl6 enable
```

diagnose ipv6 router zl6 show

Show whether flag is set.

```
diagnose ipv6 router zl6 show
```

diagnose ipv6 sit-tunnel

tunnels

This topic includes the following commands:

- [diagnose ipv6 sit-tunnel list on page 3032](#)

diagnose ipv6 sit-tunnel list

Show tunnels.

```
diagnose ipv6 sit-tunnel list
```

diagnose l2vpn evpn

EVPN debug.

This topic includes the following commands:

- [diagnose l2vpn evpn all on page 3033](#)
- [diagnose l2vpn evpn cmdb on page 3033](#)
- [diagnose l2vpn evpn events on page 3033](#)
- [diagnose l2vpn evpn fdb on page 3033](#)
- [diagnose l2vpn evpn flush on page 3033](#)
- [diagnose l2vpn evpn ha on page 3034](#)
- [diagnose l2vpn evpn macip on page 3034](#)
- [diagnose l2vpn evpn nl on page 3034](#)
- [diagnose l2vpn evpn resync on page 3034](#)
- [diagnose l2vpn evpn show on page 3034](#)
- [diagnose l2vpn evpn zebos on page 3034](#)

diagnose l2vpn evpn all

Enable/disable all EVPN debugging.

```
diagnose l2vpn evpn all
```

diagnose l2vpn evpn cmdb

Enable/disable EVPN CMDB debugging.

```
diagnose l2vpn evpn cmdb
```

diagnose l2vpn evpn events

Enable/disable EVPN events debugging.

```
diagnose l2vpn evpn events
```

diagnose l2vpn evpn fdb

Enable/disable EVPN FDB debugging.

```
diagnose l2vpn evpn fdb
```

diagnose l2vpn evpn flush

Flush EVPN local IP or MAC tables.

```
diagnose l2vpn evpn flush
```

diagnose l2vpn evpn ha

Enable/disable EVPN HA debugging.

```
diagnose l2vpn evpn ha
```

diagnose l2vpn evpn macip

Enable/disable EVPN MAC/IP debugging.

```
diagnose l2vpn evpn macip
```

diagnose l2vpn evpn nl

Enable/disable EVPN NETLINK debugging.

```
diagnose l2vpn evpn nl
```

diagnose l2vpn evpn resync

Resync EVPN local MAC tables from switch FDB.

```
diagnose l2vpn evpn resync
```

diagnose l2vpn evpn show

Show status of EVPN debugging.

```
diagnose l2vpn evpn show
```

diagnose l2vpn evpn zebos

Enable/disable EVPN ZebOS debugging.

```
diagnose l2vpn evpn zebos
```

diagnose lldp

Link Layer Description Protocol (LLDP) diagnostics.

This topic includes the following commands:

- [diagnose lldp config on page 3035](#)
- [diagnose lldp restart on page 3035](#)
- [diagnose lldp rx on page 3036](#)
- [diagnose lldp rx neighbor on page 3036](#)
- [diagnose lldp rx neighbor clear on page 3036](#)
- [diagnose lldp rx neighbor details on page 3036](#)
- [diagnose lldp rx neighbor summary on page 3036](#)
- [diagnose lldp rx port on page 3036](#)
- [diagnose lldp rx port details on page 3037](#)
- [diagnose lldp rx port neighbor on page 3037](#)
- [diagnose lldp rx port neighbor clear on page 3037](#)
- [diagnose lldp rx port neighbor details on page 3037](#)
- [diagnose lldp rx port neighbor summary on page 3037](#)
- [diagnose lldp rx port summary on page 3037](#)
- [diagnose lldp stats on page 3038](#)
- [diagnose lldp stats config on page 3038](#)
- [diagnose lldp stats crash on page 3038](#)
- [diagnose lldp stats manager on page 3038](#)
- [diagnose lldp stats rxtx on page 3038](#)
- [diagnose lldp tx on page 3038](#)
- [diagnose lldp tx port on page 3039](#)
- [diagnose lldp tx port details on page 3039](#)
- [diagnose lldp tx port summary on page 3039](#)

diagnose lldp config

Display LLDP configuration.

```
diagnose lldp config
```

diagnose lldp restart

Restart the LLDP process

```
diagnose lldp restart
```

diagnose lldp rx

Link Layer Description Protocol (LLDP) Receiver diagnostics.

```
diagnose lldp rx
```

diagnose lldp rx neighbor

Display LLDP neighbors.

```
diagnose lldp rx neighbor
```

diagnose lldp rx neighbor clear

Clear the LLDP from all ports.

```
diagnose lldp rx neighbor clear
```

diagnose lldp rx neighbor details

Display details of each LLDP neighbor.

```
diagnose lldp rx neighbor details
```

diagnose lldp rx neighbor summary

Display summary of each LLDP neighbor.

```
diagnose lldp rx neighbor summary
```

diagnose lldp rx port

Display summary information about each port with LLDP reception enabled.

```
diagnose lldp rx port
```

diagnose lldp rx port details

Display details of the LLDP enabled ports.

```
diagnose lldp rx port details
```

diagnose lldp rx port neighbor

Display information about each LLDP neighbor for one or more ports.

```
diagnose lldp rx port neighbor
```

diagnose lldp rx port neighbor clear

Clear the LLDP neighbor information for one or more ports.

```
diagnose lldp rx port neighbor clear
```

diagnose lldp rx port neighbor details

Display details of each LLDP neighbor for one or more ports.

```
diagnose lldp rx port neighbor details
```

diagnose lldp rx port neighbor summary

Display summary of each LLDP neighbor for one or more ports.

```
diagnose lldp rx port neighbor summary
```

diagnose lldp rx port summary

Display summary of the LLDP enabled ports.

```
diagnose lldp rx port summary
```

diagnose lldp stats

Display LLDP statistics.

```
diagnose lldp stats
```

diagnose lldp stats config

Display LLDP statistics for the configuration handling process.

```
diagnose lldp stats config
```

diagnose lldp stats crash

Display LLDP statistics for the crash log generating process.

```
diagnose lldp stats crash
```

diagnose lldp stats manager

Display LLDP statistics for the manager process.

```
diagnose lldp stats manager
```

diagnose lldp stats rxtx

Display LLDP statistics for the receiving and transmission process.

```
diagnose lldp stats rxtx
```

diagnose lldp tx

Link Layer Description Protocol (LLDP) Transmission diagnostics.

```
diagnose lldp tx
```

diagnose lldp tx port

Link Layer Description Protocol (LLDP) Port diagnostics.

```
diagnose lldp tx port
```

diagnose lldp tx port details

Display details of the LLDP transmission ports.

```
diagnose lldp tx port details
```

diagnose lldp tx port summary

Display summary of the LLDP transmission ports.

```
diagnose lldp tx port summary
```

diagnose log

log

This topic includes the following commands:

- [diagnose log alertmail on page 3040](#)
- [diagnose log alertmail authcode on page 3040](#)
- [diagnose log alertmail test on page 3040](#)
- [diagnose log check-empty on page 3040](#)
- [diagnose log clear-kernel-stats on page 3040](#)
- [diagnose log dummy-log on page 3041](#)
- [diagnose log dummy-log fill on page 3041](#)
- [diagnose log dummy-log remove on page 3041](#)
- [diagnose log field-enum on page 3041](#)
- [diagnose log field-list on page 3041](#)
- [diagnose log kernel-stats on page 3041](#)
- [diagnose log severity on page 3042](#)
- [diagnose log show on page 3042](#)
- [diagnose log stress-test on page 3042](#)
- [diagnose log sub-category on page 3042](#)
- [diagnose log test on page 3042](#)

- [diagnose log test-text on page 3042](#)
- [diagnose log wireless-controller on page 3043](#)

diagnose log alertmail

alertmail

```
diagnose log alertmail
```

diagnose log alertmail authcode

Send a test authentication code.

```
diagnose log alertmail authcode <recipient>
```

Parameter	Description	Type	Size
<recipient>	recipient's email address	string	

diagnose log alertmail test

Send a test alert mail.

```
diagnose log alertmail test <level> <number>
```

Parameter	Description	Type	Size
<level>	Log level number.	string	
<number>	Number of messages.	string	

diagnose log check-empty

check-empty

```
diagnose log check-empty
```

diagnose log clear-kernel-stats

Clear logging statistics.

```
diagnose log clear-kernel-stats
```


diagnose log dummy-log

dummy-log

```
diagnose log dummy-log
```

diagnose log dummy-log fill

Fill up log disk with dummy logs.

```
diagnose log dummy-log fill
```

diagnose log dummy-log remove

Remove dummy logs from log disk.

```
diagnose log dummy-log remove
```

diagnose log field-enum

field-enum

```
diagnose log field-enum
```

diagnose log field-list

field-list

```
diagnose log field-list
```

diagnose log kernel-stats

Query logging statistics.

```
diagnose log kernel-stats
```

diagnose log severity

severity

```
diagnose log severity
```

diagnose log show

Display the contents of a log file.

```
diagnose log show
```

diagnose log stress-test

stress-test

```
diagnose log stress-test
```

diagnose log sub-category

sub-category

```
diagnose log sub-category
```

diagnose log test

Test miglog.

```
diagnose log test
```

diagnose log test-text

Test miglog.

```
diagnose log test-text
```

diagnose log wireless-controller

Test wireless event log.

```
diagnose log wireless-controller
```

diagnose netlink aggregate

802.3ad link aggregation

This topic includes the following commands:

- [diagnose netlink aggregate list on page 3043](#)
- [diagnose netlink aggregate list-active on page 3043](#)
- [diagnose netlink aggregate name on page 3043](#)
- [diagnose netlink aggregate port on page 3044](#)

diagnose netlink aggregate list

list of 802.3ad link aggregation interfaces

```
diagnose netlink aggregate list
```

diagnose netlink aggregate list-active

list active 802.3ad link aggregation interfaces

```
diagnose netlink aggregate list-active <name>
```

Parameter	Description	Type	Size
<name>	aggregate name	string	

diagnose netlink aggregate name

details of a specific 802.3ad link aggregate

```
diagnose netlink aggregate name <name> <action>
```

Parameter	Description	Type	Size
<name>	aggregate name	string	
<action>	{0 s show}: Show details of a specific 802.3ad link aggregate, {1 c clear}: Clear LACPDU counters	string	

diagnose netlink aggregate port

determine which physical port a packet will exit on

```
diagnose netlink aggregate port
```

diagnose netlink backlog

UDP sockets.

This topic includes the following commands:

- [diagnose netlink backlog get on page 3044](#)
- [diagnose netlink backlog set on page 3044](#)

diagnose netlink backlog get

Show backlog.

```
diagnose netlink backlog get
```

diagnose netlink backlog set

Backlog.

```
diagnose netlink backlog set <backlog>
```

Parameter	Description	Type	Size
<backlog>	Backlog value.	string	

diagnose netlink brctl

brctl

This topic includes the following commands:

- [diagnose netlink brctl domain on page 3045](#)
- [diagnose netlink brctl list on page 3045](#)
- [diagnose netlink brctl name on page 3045](#)

diagnose netlink brctl domain

domain

```
diagnose netlink brctl domain <name> <id>
```

Parameter	Description	Type	Size
<name>	Bridge name domain_id ...	string	
<id>	id	string	

diagnose netlink brctl list

list

```
diagnose netlink brctl list
```

diagnose netlink brctl name

name

```
diagnose netlink brctl name <type> <name>
```

Parameter	Description	Type	Size
<type>	"host" or "port"	string	
<name>	name	string	

diagnose netlink device

devices

This topic includes the following commands:

- [diagnose netlink device list on page 3046](#)

diagnose netlink device list

List devices.

```
diagnose netlink device list
```

diagnose netlink dstmac

Destination MAC substitution.

This topic includes the following commands:

- [diagnose netlink dstmac flush on page 3046](#)
- [diagnose netlink dstmac list on page 3046](#)

diagnose netlink dstmac flush

flush

```
diagnose netlink dstmac flush
```

diagnose netlink dstmac list

list

```
diagnose netlink dstmac list [name]
```

Parameter	Description	Type	Size
[name]	Interface name.	string	

diagnose netlink interface

Network interfaces.

This topic includes the following commands:

- [diagnose netlink interface clear on page 3047](#)
- [diagnose netlink interface list on page 3047](#)
- [diagnose netlink interface packet-rate on page 3047](#)
- [diagnose netlink interface speed-test on page 3047](#)
- [diagnose netlink interface speed-test-result on page 3048](#)
- [diagnose netlink interface speed-test-result-clear on page 3048](#)
- [diagnose netlink interface speed-test-tunnel on page 3048](#)

diagnose netlink interface clear

Clear interface counters.

```
diagnose netlink interface clear
```

diagnose netlink interface list

List interfaces.

```
diagnose netlink interface list
```

diagnose netlink interface packet-rate

Show send/receive rate of interfaces.

```
diagnose netlink interface packet-rate
```

diagnose netlink interface speed-test

Execute speed-test on the interface.

```
diagnose netlink interface speed-test <intf-name> <server> <mode> <dry-run>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<server>	server name.	string	
<mode>	Optional. Auto(default), TCP or UDP.	string	
<dry-run>	Optional. <0> execute speed-test; <1> dry run to verify routing etc.	string	

diagnose netlink interface speed-test-result

Get speed-test result for a specific test ID.

```
diagnose netlink interface speed-test-result <test-id>
```

Parameter	Description	Type	Size
<test-id>	Test ID from executing speed-test.	string	

diagnose netlink interface speed-test-result-clear

Remove speed test results from disk.

```
diagnose netlink interface speed-test-result-clear
```

diagnose netlink interface speed-test-tunnel

Request speed-test on tunnels' underlay interfaces.

```
diagnose netlink interface speed-test-tunnel <ipsec-phase1-interface> <all | a tunnel name>
```

Parameter	Description	Type	Size
<ipsec-phase1-interface>	Interface Name.	string	
<all a tunnel name>	Specify tunnel's name or 'all'	string	

diagnose netlink intf-class

Network interface class.

This topic includes the following commands:

- [diagnose netlink intf-class list on page 3049](#)

diagnose netlink intf-class list

list

```
diagnose netlink intf-class list <string>
```

Parameter	Description	Type	Size
<string>	Interface name.	string	

diagnose netlink intf-qdisc

Network interface qdisc.

This topic includes the following commands:

- [diagnose netlink intf-qdisc list on page 3049](#)

diagnose netlink intf-qdisc list

list

```
diagnose netlink intf-qdisc list <string>
```

Parameter	Description	Type	Size
<string>	Interface name.	string	

diagnose netlink qlen

Interface queue length.

This topic includes the following commands:

- [diagnose netlink qlen get on page 3050](#)
- [diagnose netlink qlen set on page 3050](#)

diagnose netlink qlen get

Get queue length.

```
diagnose netlink qlen get <intf-name>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	

diagnose netlink qlen set

Queue length.

```
diagnose netlink qlen set <intf-name> <len_integer>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<len_integer>	Length value.	string	

diagnose netlink redundant

redundant interfaces

This topic includes the following commands:

- [diagnose netlink redundant list on page 3050](#)
- [diagnose netlink redundant name on page 3051](#)

diagnose netlink redundant list

list of redundant interfaces

```
diagnose netlink redundant list
```

diagnose netlink redundant name

details of a specific redundant interface

```
diagnose netlink redundant name <name>
```

Parameter	Description	Type	Size
<name>	redundant interface name	string	

diagnose nodejs

Node.JS web server diagnostics.

This topic includes the following commands:

- [diagnose nodejs health-check on page 3051](#)
- [diagnose nodejs health-check ping on page 3051](#)
- [diagnose nodejs logs on page 3052](#)
- [diagnose nodejs logs delete on page 3052](#)
- [diagnose nodejs logs list on page 3052](#)
- [diagnose nodejs logs show on page 3052](#)
- [diagnose nodejs logs show-all on page 3052](#)
- [diagnose nodejs performance on page 3053](#)
- [diagnose nodejs performance mass-ztna-event-logs on page 3053](#)
- [diagnose nodejs process on page 3053](#)
- [diagnose nodejs process restart on page 3053](#)

diagnose nodejs health-check

Node.JS health check commands.

```
diagnose nodejs health-check
```

diagnose nodejs health-check ping

Send HTTP request to Node.JS, and check if Node.JS can handle HTTP request.

```
diagnose nodejs health-check ping
```

diagnose nodejs logs

Show/List Node.JS debug log.

```
diagnose nodejs logs
```

diagnose nodejs logs delete

Delete one of the Node.JS debug log files. Use log sequence number as an argument.

```
diagnose nodejs logs delete <log sequence number>
```

Parameter	Description	Type	Size
<log sequence number>	Log sequence number.	string	

diagnose nodejs logs list

List all of the Node.JS debug log files.

```
diagnose nodejs logs list
```

diagnose nodejs logs show

Show one of the Node.JS debug logs files. Use log sequence number as an argument.

```
diagnose nodejs logs show <log sequence number>
```

Parameter	Description	Type	Size
<log sequence number>	Log sequence number.	string	

diagnose nodejs logs show-all

Show all of the Node.JS debug log files.

```
diagnose nodejs logs show-all
```

diagnose nodejs performance

Performance testing for Node.js.

```
diagnose nodejs performance
```

diagnose nodejs performance mass-ztna-event-logs

Generate thousands of ZTNA tag update events.

```
diagnose nodejs performance mass-ztna-event-logs
```

diagnose nodejs process

Actions to Node.JS process.

```
diagnose nodejs process
```

diagnose nodejs process restart

Send SIGKILL and restart Node.JS.

```
diagnose nodejs process restart
```

diagnose oci

Oracle Cloud Infrastructure platform diagnose commands.

This topic includes the following commands:

- [diagnose oci pubkey on page 3053](#)

diagnose oci pubkey

Display OCI public key information.

```
diagnose oci pubkey <name>
```

Parameter	Description	Type	Size
<name>	OCI SDN connector name	string	

diagnose on-demand-sniffer

On-demand sniffer command.

This topic includes the following commands:

- [diagnose on-demand-sniffer delete-results](#) on page 3054
- [diagnose on-demand-sniffer list](#) on page 3054
- [diagnose on-demand-sniffer start](#) on page 3054
- [diagnose on-demand-sniffer stop](#) on page 3055

diagnose on-demand-sniffer delete-results

Delete files associated with an on-demand sniffer. Does not delete the config entry.

```
diagnose on-demand-sniffer delete-results <mkey/name>
```

Parameter	Description	Type	Size
<mkey/name>	Mkey/name of on-demand sniffer.	string	

diagnose on-demand-sniffer list

List on-demand sniffers and its info.

```
diagnose on-demand-sniffer list <mkey/name>
```

Parameter	Description	Type	Size
<mkey/name>	Mkey/name of on-demand sniffer.	string	

diagnose on-demand-sniffer start

Start an on-demand sniffer.

```
diagnose on-demand-sniffer start <mkey/name>
```

Parameter	Description	Type	Size
<mkey/name>	Mkey/name of on-demand sniffer.	string	

diagnose on-demand-sniffer stop

Stop an on-demand sniffer.

```
diagnose on-demand-sniffer stop <mkey/name>
```

Parameter	Description	Type	Size
<mkey/name>	Mkey/name of on-demand sniffer.	string	

diagnose radiusd

RADIUS daemon diagnostic commands.

This topic includes the following commands:

- [diagnose radiusd test on page 3055](#)

diagnose radiusd test

Send test command to RADIUS daemon.

```
diagnose radiusd test <level>
```

Parameter	Description	Type	Size
<level>	Test level (integer).	string	

diagnose report

report

This topic includes the following commands:

- [diagnose report clear-filter on page 3056](#)
- [diagnose report dataset on page 3056](#)
- [diagnose report filter on page 3056](#)

- [diagnose report min-points on page 3056](#)
- [diagnose report ondemand-table on page 3056](#)
- [diagnose report sql on page 3056](#)
- [diagnose report time on page 3057](#)
- [diagnose report top-n on page 3057](#)

diagnose report clear-filter

clear-filter

```
diagnose report clear-filter
```

diagnose report dataset

dataset

```
diagnose report dataset
```

diagnose report filter

filter

```
diagnose report filter
```

diagnose report min-points

min-points

```
diagnose report min-points
```

diagnose report ondemand-table

ondemand-table

```
diagnose report ondemand-table
```

diagnose report sql

sql


```
diagnose report sql
```

diagnose report time

time

```
diagnose report time
```

diagnose report top-n

top-n

```
diagnose report top-n
```

diagnose report-runner

Report Runner service.

This topic includes the following commands:

- [diagnose report-runner clean on page 3057](#)
- [diagnose report-runner trigger on page 3057](#)
- [diagnose report-runner trigger security-rating-reports on page 3058](#)
- [diagnose report-runner vuln-clean on page 3058](#)
- [diagnose report-runner vuln-read on page 3058](#)

diagnose report-runner clean

Delete all Report Runner results.

```
diagnose report-runner clean
```

diagnose report-runner trigger

Execute a report.

```
diagnose report-runner trigger
```

diagnose report-runner trigger security-rating-reports

Execute the Security Rating reports (Security Posture, Fabric Coverage, Optimization).

```
diagnose report-runner trigger security-rating-reports
```

diagnose report-runner vuln-clean

Delete critical vulnerability results.

```
diagnose report-runner vuln-clean
```

diagnose report-runner vuln-read

View critical vulnerability results.

```
diagnose report-runner vuln-read
```

diagnose report-runner-v2

Report Runner v2 service.

This topic includes the following commands:

- [diagnose report-runner-v2 clean on page 3058](#)
- [diagnose report-runner-v2 security-rating on page 3059](#)
- [diagnose report-runner-v2 security-rating clean on page 3059](#)
- [diagnose report-runner-v2 security-rating reset-trigger on page 3059](#)
- [diagnose report-runner-v2 security-rating trigger on page 3059](#)
- [diagnose report-runner-v2 security-rating trigger-check on page 3059](#)

diagnose report-runner-v2 clean

Clean all Report Runner V2 results.

```
diagnose report-runner-v2 clean
```

diagnose report-runner-v2 security-rating

Security Rating.

```
diagnose report-runner-v2 security-rating
```

diagnose report-runner-v2 security-rating clean

Delete all Security Rating v2 results.

```
diagnose report-runner-v2 security-rating clean
```

diagnose report-runner-v2 security-rating reset-trigger

Reset the automatic trigger timeout.

```
diagnose report-runner-v2 security-rating reset-trigger
```

diagnose report-runner-v2 security-rating trigger

Force trigger a full run.

```
diagnose report-runner-v2 security-rating trigger
```

diagnose report-runner-v2 security-rating trigger-check

Trigger a specific check.

```
diagnose report-runner-v2 security-rating trigger-check <check>
```

Parameter	Description	Type	Size
<check>	Check to trigger.	string	

diagnose rssso

RSSO diagnostic commands.

This topic includes the following commands:

- [diagnose rso delete on page 3060](#)
- [diagnose rso delete ip on page 3060](#)
- [diagnose rso delete ip6 on page 3060](#)
- [diagnose rso query on page 3060](#)
- [diagnose rso query carrier-endpoint on page 3061](#)
- [diagnose rso query ip on page 3061](#)
- [diagnose rso query ip6 on page 3061](#)
- [diagnose rso query rso-key on page 3061](#)
- [diagnose rso resync on page 3062](#)
- [diagnose rso resync fgcp on page 3062](#)
- [diagnose rso resync fgsp on page 3062](#)

diagnose rso delete

Delete entries in RSSO database.

```
diagnose rso delete
```

diagnose rso delete ip

delete by IP address.

```
diagnose rso delete ip <ip>
```

Parameter	Description	Type	Size
<ip>	IP address to delete.	string	

diagnose rso delete ip6

delete by IP6 address.

```
diagnose rso delete ip6 <ip6>
```

Parameter	Description	Type	Size
<ip6>	IP6 address to delete.	string	

diagnose rso query

Query RSSO database.

```
diagnose rso query
```

diagnose rso query carrier-endpoint

Query by End Point.

```
diagnose rso query carrier-endpoint <endpoint> <ip>
```

Parameter	Description	Type	Size
<endpoint>	End Point to query.	string	
<ip>	IP address of TFTP server to upload results (optional).	string	

diagnose rso query ip

Query by IP address.

```
diagnose rso query ip <ip> <ip>
```

Parameter	Description	Type	Size
<ip>	IP address to query.	string	
<ip>	IP address of TFTP server to upload results (optional).	string	

diagnose rso query ip6

Query by IP6 address.

```
diagnose rso query ip6 <ip6> <ip>
```

Parameter	Description	Type	Size
<ip6>	IP6 address to query.	string	
<ip>	IP address of TFTP server to upload results (optional).	string	

diagnose rso query rso-key

Query by RSSO key.

```
diagnose rso query rso-key <name> <ip>
```

Parameter	Description	Type	Size
<name>	RSSO key to query.	string	
<ip>	IP address of TFTP server to upload results (optional).	string	

diagnose rso resync

Resync RSSO database in the vdom from its peer.

```
diagnose rso resync
```

diagnose rso resync fgcp

Resync from FGCP peer.

```
diagnose rso resync fgcp
```

diagnose rso resync fgsp

Resync from FGSP peer.

```
diagnose rso resync fgsp <vdom>
```

Parameter	Description	Type	Size
<vdom>	Vdom name.	string	

diagnose saas

SaaS diagnose commands.

This topic includes the following commands:

- [diagnose saas reload on page 3063](#)
- [diagnose saas show on page 3063](#)
- [diagnose saas show apps on page 3063](#)
- [diagnose saas show details on page 3063](#)
- [diagnose saas show status on page 3063](#)

diagnose saas reload

Reload SaaS database.

```
diagnose saas reload
```

diagnose saas show

Show SaaS database.

```
diagnose saas show
```

diagnose saas show apps

Show SaaS database application list.

```
diagnose saas show apps
```

diagnose saas show details

Show SaaS database details.

```
diagnose saas show details
```

diagnose saas show status

Show SaaS database status.

```
diagnose saas show status
```

diagnose settings

settings

This topic includes the following commands:

- [diagnose settings info on page 3064](#)
- [diagnose settings reset on page 3064](#)

diagnose settings info

Show all diagnose settings.

```
diagnose settings info
```

diagnose settings reset

Reset all diagnose settings.

```
diagnose settings reset
```

diagnose sladb

Service Level Agreement Database.

This topic includes the following commands:

- [diagnose sladb domain-list on page 3064](#)
- [diagnose sladb protocol-list on page 3064](#)
- [diagnose sladb target-list on page 3065](#)

diagnose sladb domain-list

List all domains under a specific target predefined by FortiGuard.

```
diagnose sladb domain-list <target-name>
```

Parameter	Description	Type	Size
<target-name>	Target-Name	string	

diagnose sladb protocol-list

List all protocols under specific target and domain predefined by FortiGuard.

```
diagnose sladb protocol-list <target-name> <domain-name>
```


Parameter	Description	Type	Size
<target-name>	Target-Name	string	
<domain-name>	Domain-Name	string	

diagnose sladb target-list

List all targets predefined by FortiGuard.

```
diagnose sladb target-list
```

diagnose sniffer

Sniffer command.

This topic includes the following commands:

- [diagnose sniffer dpdk on page 3065](#)
- [diagnose sniffer migsock on page 3066](#)
- [diagnose sniffer migsock debug-trace on page 3066](#)
- [diagnose sniffer migsock debug-trace disable on page 3066](#)
- [diagnose sniffer migsock debug-trace enable on page 3067](#)
- [diagnose sniffer migsock filter on page 3067](#)
- [diagnose sniffer migsock ssl-trace on page 3067](#)
- [diagnose sniffer migsock ssl-trace disable on page 3067](#)
- [diagnose sniffer migsock ssl-trace enable on page 3067](#)
- [diagnose sniffer migsock start on page 3067](#)
- [diagnose sniffer migsock timestamp on page 3068](#)
- [diagnose sniffer migsock timestamp disable on page 3068](#)
- [diagnose sniffer migsock timestamp enable on page 3068](#)
- [diagnose sniffer packet on page 3068](#)

diagnose sniffer dpdk

Sniff packets on Rx/Tx of DPDK interfaces. (DPDK Sniffing Mode)

```
diagnose sniffer dpdk <interface> <filter> <verbose> <count> <tsformat> <frame size>
```

Parameter	Description	Type	Size
<interface>	Network interface to sniff (or "any").	string	
<filter>	Flexible logical filters for sniffer (or "none"). For example: To print UDP 1812 traffic between forti1 and either forti2 or forti3 'udp and port 1812 and host forti1 and (forti2 or forti3)'	string	
<verbose>	1: print header of packets 2: print header and data from ip of packets 3: print header and data from ethernet of packets (if available) 4: print header of packets with interface name 5: print header and data from ip of packets with interface name 6: print header and data from ethernet of packets (if available) with intf name	string	
<count>	Sniffer count.	string	
<tsformat>	Format of timestamp. a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms otherwise: relative to the start of sniffing, ss.ms	string	
<frame size>	Set the frame size that is printed before truncation. Defaults to the interface MTU.	string	

diagnose sniffer migsock

Sniff migsock packets.

```
diagnose sniffer migsock
```

diagnose sniffer migsock debug-trace

Enable/disable debug trace.

```
diagnose sniffer migsock debug-trace
```

diagnose sniffer migsock debug-trace disable

Disable debug trace.

```
diagnose sniffer migsock debug-trace disable
```

diagnose sniffer migsock debug-trace enable

Enable debug trace.

```
diagnose sniffer migsock debug-trace enable
```

diagnose sniffer migsock filter

Filter flow.

```
diagnose sniffer migsock filter <filter>
```

Parameter	Description	Type	Size
<filter>	Filter string.	string	

diagnose sniffer migsock ssl-trace

Enable/disable SSL trace.

```
diagnose sniffer migsock ssl-trace
```

diagnose sniffer migsock ssl-trace disable

Disable SSL trace.

```
diagnose sniffer migsock ssl-trace disable
```

diagnose sniffer migsock ssl-trace enable

Enable SSL trace.

```
diagnose sniffer migsock ssl-trace enable
```

diagnose sniffer migsock start

Start sniffer.

```
diagnose sniffer migsock start
```

diagnose sniffer migsock timestamp

Enable/disable timestamp trace.

```
diagnose sniffer migsock timestamp
```

diagnose sniffer migsock timestamp disable

Disable timestamp trace.

```
diagnose sniffer migsock timestamp disable
```

diagnose sniffer migsock timestamp enable

Enable timestamp trace.

```
diagnose sniffer migsock timestamp enable
```

diagnose sniffer packet

Sniff packets.

```
diagnose sniffer packet <interface> <filter> <verbose> <count> <tsformat> <frame size>
```

Parameter	Description	Type	Size
<interface>	Network interface to sniff (or "any").	string	
<filter>	Flexible logical filters for sniffer (or "none"). For example: To print UDP 1812 traffic between forti1 and either forti2 or forti3 'udp and port 1812 and host forti1 and (forti2 or forti3)'	string	
<verbose>	1: print header of packets 2: print header and data from ip of packets 3: print header and data from ethernet of packets (if available) 4: print header of packets with interface name 5: print header and data from ip of packets with interface name 6: print header and data from ethernet of packets (if available) with intf name	string	
<count>	Sniffer count.	string	

Parameter	Description	Type	Size
<tsformat>	Format of timestamp. a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms otherwise: relative to the start of sniffing, ss.ms	string	
<frame size>	Set the frame size that is printed before truncation. Defaults to the interface MTU.	string	

diagnose snmp ip

Some IP stats.

This topic includes the following commands:

- [diagnose snmp ip frags on page 3069](#)
- [diagnose snmp ip icmp on page 3069](#)
- [diagnose snmp ip ip on page 3070](#)
- [diagnose snmp ip tcp on page 3070](#)
- [diagnose snmp ip udp on page 3070](#)

diagnose snmp ip frags

Fragmentation and reassembly info.

```
diagnose snmp ip frags <rate>
```

Parameter	Description	Type	Size
<rate>	Fragmentation and reassembly info per second	string	

diagnose snmp ip icmp

ICMP related statistics info.

```
diagnose snmp ip icmp <rate>
```

Parameter	Description	Type	Size
<rate>	ICMP related statistics per second	string	

diagnose snmp ip ip

IP related statistics info.

```
diagnose snmp ip ip <rate>
```

Parameter	Description	Type	Size
<rate>	IP related statistics per second	string	

diagnose snmp ip tcp

TCP related statistics info.

```
diagnose snmp ip tcp
```

diagnose snmp ip udp

UDP related statistics info.

```
diagnose snmp ip udp <rate>
```

Parameter	Description	Type	Size
<rate>	UDP related statistics per second	string	

diagnose snmp ip6

Some IPv6 stats.

This topic includes the following commands:

- [diagnose snmp ip6 frags on page 3070](#)
- [diagnose snmp ip6 icmp6 on page 3071](#)
- [diagnose snmp ip6 ip6 on page 3071](#)
- [diagnose snmp ip6 udp6 on page 3071](#)

diagnose snmp ip6 frags

Fragmentation and reassembly info.

```
diagnose snmp ip6 frags <rate>
```

Parameter	Description	Type	Size
<rate>	Fragmentation and reassembly info per second	string	

diagnose snmp ip6 icmp6

ICMP related statistics info.

```
diagnose snmp ip6 icmp6 <rate>
```

Parameter	Description	Type	Size
<rate>	ICMP related statistics per second	string	

diagnose snmp ip6 ip6

IP related statistics info.

```
diagnose snmp ip6 ip6 <rate>
```

Parameter	Description	Type	Size
<rate>	IPv6 related statistics per second	string	

diagnose snmp ip6 udp6

UDP related statistics info.

```
diagnose snmp ip6 udp6 <rate>
```

Parameter	Description	Type	Size
<rate>	UDP related statistics per second	string	

diagnose snmp net

Some network statistics.

This topic includes the following commands:

- [diagnose snmp net stat on page 3072](#)

diagnose snmp net stat

Network statistics.

```
diagnose snmp net stat
```

diagnose snmp trap

SNMP trap diagnostics.

This topic includes the following commands:

- [diagnose snmp trap send on page 3072](#)

diagnose snmp trap send

Generate a trap event.

```
diagnose snmp trap send
```

diagnose switch-controller

Fortiswitch controller.

This topic includes the following commands:

- [diagnose switch-controller flow-collector on page 3076](#)
- [diagnose switch-controller flow-collector status on page 3076](#)
- [diagnose switch-controller mac-cache on page 3076](#)
- [diagnose switch-controller mac-cache filter on page 3076](#)
- [diagnose switch-controller mac-cache filter clear on page 3076](#)
- [diagnose switch-controller mac-cache filter intf-name on page 3076](#)
- [diagnose switch-controller mac-cache filter mac on page 3077](#)
- [diagnose switch-controller mac-cache filter vlan-id on page 3077](#)
- [diagnose switch-controller mac-cache show on page 3077](#)
- [diagnose switch-controller mac-device on page 3077](#)
- [diagnose switch-controller mac-device cache on page 3077](#)
- [diagnose switch-controller mac-device dynamic on page 3078](#)
- [diagnose switch-controller mac-device nac on page 3078](#)
- [diagnose switch-controller mac-device nac known on page 3078](#)

- [diagnose switch-controller mac-device nac onboarding on page 3078](#)
- [diagnose switch-controller nac-tag on page 3078](#)
- [diagnose switch-controller nac-tag add on page 3078](#)
- [diagnose switch-controller nac-tag delete on page 3079](#)
- [diagnose switch-controller nac-tag get on page 3079](#)
- [diagnose switch-controller restart-daemon on page 3079](#)
- [diagnose switch-controller restart-daemon acd on page 3079](#)
- [diagnose switch-controller restart-daemon swtpd on page 3079](#)
- [diagnose switch-controller switch-info on page 3080](#)
- [diagnose switch-controller switch-info 802.1X on page 3080](#)
- [diagnose switch-controller switch-info 802.1X-dacl on page 3080](#)
- [diagnose switch-controller switch-info acl-counters on page 3080](#)
- [diagnose switch-controller switch-info arp-inspection on page 3081](#)
- [diagnose switch-controller switch-info arp-inspection stats on page 3081](#)
- [diagnose switch-controller switch-info arp-inspection stats-clear on page 3081](#)
- [diagnose switch-controller switch-info bpdu-guard-status on page 3081](#)
- [diagnose switch-controller switch-info dhcp-snooping on page 3082](#)
- [diagnose switch-controller switch-info dhcp-snooping database on page 3082](#)
- [diagnose switch-controller switch-info dhcp-snooping status on page 3082](#)
- [diagnose switch-controller switch-info fan on page 3082](#)
- [diagnose switch-controller switch-info flapguard on page 3082](#)
- [diagnose switch-controller switch-info flapguard status on page 3083](#)
- [diagnose switch-controller switch-info flow-tracking on page 3083](#)
- [diagnose switch-controller switch-info flow-tracking flows on page 3083](#)
- [diagnose switch-controller switch-info flow-tracking flows-raw on page 3083](#)
- [diagnose switch-controller switch-info flow-tracking statistics on page 3084](#)
- [diagnose switch-controller switch-info igmp-snooping on page 3084](#)
- [diagnose switch-controller switch-info igmp-snooping group on page 3084](#)
- [diagnose switch-controller switch-info igmp-snooping status on page 3084](#)
- [diagnose switch-controller switch-info ip-source-guard on page 3085](#)
- [diagnose switch-controller switch-info ip-source-guard hardware on page 3085](#)
- [diagnose switch-controller switch-info lldp on page 3085](#)
- [diagnose switch-controller switch-info lldp neighbors-detail on page 3085](#)
- [diagnose switch-controller switch-info lldp neighbors-summary on page 3086](#)
- [diagnose switch-controller switch-info lldp stats on page 3086](#)
- [diagnose switch-controller switch-info loop-guard on page 3086](#)
- [diagnose switch-controller switch-info mac-limit-violations on page 3086](#)
- [diagnose switch-controller switch-info mac-limit-violations all on page 3087](#)
- [diagnose switch-controller switch-info mac-limit-violations interface on page 3087](#)
- [diagnose switch-controller switch-info mac-limit-violations vlan on page 3087](#)
- [diagnose switch-controller switch-info mac-table on page 3087](#)
- [diagnose switch-controller switch-info mclag on page 3088](#)
- [diagnose switch-controller switch-info mclag icl on page 3088](#)

- [diagnose switch-controller switch-info mclag list on page 3088](#)
- [diagnose switch-controller switch-info mclag peer-consistency-check on page 3088](#)
- [diagnose switch-controller switch-info mirror on page 3089](#)
- [diagnose switch-controller switch-info mirror status on page 3089](#)
- [diagnose switch-controller switch-info modules on page 3089](#)
- [diagnose switch-controller switch-info modules detail on page 3089](#)
- [diagnose switch-controller switch-info modules limits on page 3090](#)
- [diagnose switch-controller switch-info modules status on page 3090](#)
- [diagnose switch-controller switch-info modules summary on page 3090](#)
- [diagnose switch-controller switch-info option82-mapping on page 3090](#)
- [diagnose switch-controller switch-info option82-mapping snooping on page 3091](#)
- [diagnose switch-controller switch-info option82-mapping snooping ascii on page 3091](#)
- [diagnose switch-controller switch-info option82-mapping snooping hex on page 3091](#)
- [diagnose switch-controller switch-info pdu-counters-list on page 3091](#)
- [diagnose switch-controller switch-info poe on page 3092](#)
- [diagnose switch-controller switch-info poe detail on page 3092](#)
- [diagnose switch-controller switch-info poe summary on page 3092](#)
- [diagnose switch-controller switch-info port-properties on page 3092](#)
- [diagnose switch-controller switch-info port-stats on page 3093](#)
- [diagnose switch-controller switch-info qos-stats on page 3093](#)
- [diagnose switch-controller switch-info rpvst on page 3093](#)
- [diagnose switch-controller switch-info status on page 3093](#)
- [diagnose switch-controller switch-info stp on page 3094](#)
- [diagnose switch-controller switch-info trunk on page 3094](#)
- [diagnose switch-controller switch-info trunk config on page 3094](#)
- [diagnose switch-controller switch-info trunk status on page 3094](#)
- [diagnose switch-controller switch-recommendation on page 3095](#)
- [diagnose switch-controller switch-recommendation bios-compatibility-check on page 3095](#)
- [diagnose switch-controller switch-recommendation check-fortilink-link-redundancy on page 3095](#)
- [diagnose switch-controller switch-recommendation check-isl-icl-link-redundancy on page 3095](#)
- [diagnose switch-controller switch-recommendation check-isl-link-redundancy on page 3096](#)
- [diagnose switch-controller switch-recommendation clear-dhcp-opt43-key on page 3096](#)
- [diagnose switch-controller switch-recommendation config-dhcp-opt43-key on page 3097](#)
- [diagnose switch-controller switch-recommendation disable-auto-config-poe-status on page 3097](#)
- [diagnose switch-controller switch-recommendation disable-bounce-quarantine-link on page 3097](#)
- [diagnose switch-controller switch-recommendation disable-poe-pre-standard-detection on page 3097](#)
- [diagnose switch-controller switch-recommendation disable-stp-state-topology on page 3098](#)
- [diagnose switch-controller switch-recommendation enable-auto-config-poe-status on page 3098](#)
- [diagnose switch-controller switch-recommendation enable-bounce-quarantine-link on page 3098](#)
- [diagnose switch-controller switch-recommendation enable-poe-pre-standard-detection on page 3098](#)
- [diagnose switch-controller switch-recommendation enable-stp-state-topology on page 3099](#)
- [diagnose switch-controller switch-recommendation fabric-lockdown-check on page 3099](#)
- [diagnose switch-controller switch-recommendation fabric-lockdown-disable on page 3099](#)

- [diagnose switch-controller switch-recommendation fabric-lockdown-enable on page 3100](#)
- [diagnose switch-controller switch-recommendation get-mclag-tier1-candidate on page 3100](#)
- [diagnose switch-controller switch-recommendation get-mclag-tier2-candidate on page 3100](#)
- [diagnose switch-controller switch-recommendation get-mclag-tier3-candidate on page 3101](#)
- [diagnose switch-controller switch-recommendation is-fortilink-capacity-exceeded on page 3101](#)
- [diagnose switch-controller switch-recommendation is-switch-dual-homed on page 3101](#)
- [diagnose switch-controller switch-recommendation lock-down-topo-lldp-profile on page 3102](#)
- [diagnose switch-controller switch-recommendation pse-check on page 3102](#)
- [diagnose switch-controller switch-recommendation pse-config on page 3102](#)
- [diagnose switch-controller switch-recommendation set-tier-plus-mclag-icl on page 3103](#)
- [diagnose switch-controller switch-recommendation set-tier1-mclag-icl on page 3103](#)
- [diagnose switch-controller switch-recommendation tunnel-mode-settings on page 3103](#)
- [diagnose switch-controller switch-recommendation unlock-topo-lldp-profile on page 3104](#)
- [diagnose switch-controller system-info on page 3104](#)
- [diagnose switch-controller system-info show on page 3104](#)
- [diagnose switch-controller telemetry on page 3104](#)
- [diagnose switch-controller telemetry show on page 3104](#)
- [diagnose switch-controller telemetry show mac-stats on page 3105](#)
- [diagnose switch-controller telemetry show mac-stats switch on page 3105](#)
- [diagnose switch-controller telemetry show switch on page 3105](#)
- [diagnose switch-controller telemetry show switch-port on page 3105](#)
- [diagnose switch-controller topology on page 3106](#)
- [diagnose switch-controller topology reset on page 3106](#)
- [diagnose switch-controller topology reset fortalink-flag on page 3106](#)
- [diagnose switch-controller topology reset isl-peer-flag on page 3106](#)
- [diagnose switch-controller topology set on page 3106](#)
- [diagnose switch-controller topology set fortalink-flag on page 3107](#)
- [diagnose switch-controller topology set isl-peer-flag on page 3107](#)
- [diagnose switch-controller traffic-capture on page 3107](#)
- [diagnose switch-controller traffic-capture show on page 3107](#)
- [diagnose switch-controller traffic-capture start on page 3107](#)
- [diagnose switch-controller traffic-capture stop on page 3108](#)
- [diagnose switch-controller trigger on page 3108](#)
- [diagnose switch-controller trigger config-sync on page 3108](#)
- [diagnose switch-controller trigger mac-sync on page 3108](#)
- [diagnose switch-controller trigger nac-mac-cache-sync on page 3109](#)
- [diagnose switch-controller trigger reset-hardware-counters on page 3109](#)
- [diagnose switch-controller trigger restore-hardware-counters on page 3109](#)
- [diagnose switch-controller tunnel-status on page 3109](#)

diagnose switch-controller flow-collector

Flow collector.

```
diagnose switch-controller flow-collector
```

diagnose switch-controller flow-collector status

Display flow collector status.

```
diagnose switch-controller flow-collector status
```

diagnose switch-controller mac-cache

Mac cache.

```
diagnose switch-controller mac-cache
```

diagnose switch-controller mac-cache filter

Filter to dump devices connected to managed FortiSwitch.

```
diagnose switch-controller mac-cache filter
```

diagnose switch-controller mac-cache filter clear

Clear the configured device filter.

```
diagnose switch-controller mac-cache filter clear
```

diagnose switch-controller mac-cache filter intf-name

Device filter interface name.

```
diagnose switch-controller mac-cache filter intf-name <intf-name>
```

Parameter	Description	Type	Size
<intf-name>	Managed FortiSwitch interface name on which the device is connected.	string	

diagnose switch-controller mac-cache filter mac

Device filter MAC Address.

```
diagnose switch-controller mac-cache filter mac <mac>
```

Parameter	Description	Type	Size
<mac>	MAC Address of device(XX:XX:XX:XX:XX:XX).	string	

diagnose switch-controller mac-cache filter vlan-id

Device filter VLAN ID.

```
diagnose switch-controller mac-cache filter vlan-id <vlan-id>
```

Parameter	Description	Type	Size
<vlan-id>	Managed FortiSwitch VLAN of device.	string	

diagnose switch-controller mac-cache show

Show running clients.

```
diagnose switch-controller mac-cache show <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller mac-device

MAC devices.

```
diagnose switch-controller mac-device
```

diagnose switch-controller mac-device cache

Event cached MAC address.

```
diagnose switch-controller mac-device cache
```

diagnose switch-controller mac-device dynamic

Display detected DPP devices which matches dynamic port policy.

```
diagnose switch-controller mac-device dynamic
```

diagnose switch-controller mac-device nac

Display NAC devices.

```
diagnose switch-controller mac-device nac
```

diagnose switch-controller mac-device nac known

Display detected NAC devices which matches NAC policy.

```
diagnose switch-controller mac-device nac known
```

diagnose switch-controller mac-device nac onboarding

Display onboarding NAC devices with no matching NAC policy.

```
diagnose switch-controller mac-device nac onboarding
```

diagnose switch-controller nac-tag

Add, remove, or show MAC from NAC dynamic firewall tag.

```
diagnose switch-controller nac-tag
```

diagnose switch-controller nac-tag add

Add MAC to dynamic NAC tag.

```
diagnose switch-controller nac-tag add <tag> <mac>
```

Parameter	Description	Type	Size
<tag>	Firewall tag.	string	
<mac>	MAC address	string	

diagnose switch-controller nac-tag delete

Delete MAC from dynamic NAC tag.

```
diagnose switch-controller nac-tag delete <tag> <mac>
```

Parameter	Description	Type	Size
<tag>	Firewall tag.	string	
<mac>	MAC address	string	

diagnose switch-controller nac-tag get

Show all MACs associated with dynamic NAC tag.

```
diagnose switch-controller nac-tag get <tag>
```

Parameter	Description	Type	Size
<tag>	Firewall tag.	string	

diagnose switch-controller restart-daemon

Restart switch controller daemons.

```
diagnose switch-controller restart-daemon
```

diagnose switch-controller restart-daemon acd

Restart switch-controller daemon.

```
diagnose switch-controller restart-daemon acd
```

diagnose switch-controller restart-daemon swtpd

Restart switch-controller daemon in FortiSwitch device.

```
diagnose switch-controller restart-daemon swtpd <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info

Switch information.

```
diagnose switch-controller switch-info
```

diagnose switch-controller switch-info 802.1X

Managed FortiSwitch port 802.1X status.

```
diagnose switch-controller switch-info 802.1X <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for 802.1X status.	string	

diagnose switch-controller switch-info 802.1X-dacl

Managed FortiSwitch port 802.1X dynamic ACL status.

```
diagnose switch-controller switch-info 802.1X-dacl <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for 802.1X dacl status.	string	

diagnose switch-controller switch-info acl-counters

Managed FortiSwitch port ACL counters.

```
diagnose switch-controller switch-info acl-counters <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller switch-info arp-inspection

Managed FortiSwitch ARP inspection interface list.

```
diagnose switch-controller switch-info arp-inspection
```

diagnose switch-controller switch-info arp-inspection stats

Show ARP inspection statistics.

```
diagnose switch-controller switch-info arp-inspection stats <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info arp-inspection stats-clear

Clear ARP inspection statistics.

```
diagnose switch-controller switch-info arp-inspection stats-clear <vlan-id> <switch>
```

Parameter	Description	Type	Size
<vlan-id>	Managed FortiSwitch VLAN of interest for MAC address list.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info bpdu-guard-status

Managed FortiSwitch STP BPDU guard status.

```
diagnose switch-controller switch-info bpdu-guard-status <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info dhcp-snooping

Managed FortiSwitch DHCP snooping interface list.

```
diagnose switch-controller switch-info dhcp-snooping
```

diagnose switch-controller switch-info dhcp-snooping database

DHCP snooping database details.

```
diagnose switch-controller switch-info dhcp-snooping database <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info dhcp-snooping status

DHCP snooping status.

```
diagnose switch-controller switch-info dhcp-snooping status <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info fan

List fan status.

```
diagnose switch-controller switch-info fan <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info flapguard

Managed FortiSwitch flap guard.

```
diagnose switch-controller switch-info flapguard
```

diagnose switch-controller switch-info flapguard status

List flapguard status.

```
diagnose switch-controller switch-info flapguard status <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info flow-tracking

Managed FortiSwitch flow information.

```
diagnose switch-controller switch-info flow-tracking
```

diagnose switch-controller switch-info flow-tracking flows

Flow record data.

```
diagnose switch-controller switch-info flow-tracking flows <count> <ip/subnet> <switch> <port>
```

Parameter	Description	Type	Size
<count>	Specify record count or all for query response.	string	
<ip/subnet>	Specify IP address/Subnet(Class IP/Netmask) or all.	string	
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port.	string	

diagnose switch-controller switch-info flow-tracking flows-raw

Flow raw record data.

```
diagnose switch-controller switch-info flow-tracking flows-raw <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info flow-tracking statistics

Flow statistics data.

```
diagnose switch-controller switch-info flow-tracking statistics <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info igmp-snooping

IGMP snooping information.

```
diagnose switch-controller switch-info igmp-snooping
```

diagnose switch-controller switch-info igmp-snooping group

Managed FortiSwitch IGMP snooping learned groups list.

```
diagnose switch-controller switch-info igmp-snooping group <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info igmp-snooping status

Managed FortiSwitch IGMP snooping status.

```
diagnose switch-controller switch-info igmp-snooping status <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info ip-source-guard

Managed FortiSwitch source guard information in hardware.

```
diagnose switch-controller switch-info ip-source-guard
```

diagnose switch-controller switch-info ip-source-guard hardware

Managed FortiSwitch IP source guard information in hardware.

```
diagnose switch-controller switch-info ip-source-guard hardware <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info lldp

LLDP-related information.

```
diagnose switch-controller switch-info lldp
```

diagnose switch-controller switch-info lldp neighbors-detail

LLDP neighbor detail.

```
diagnose switch-controller switch-info lldp neighbors-detail <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller switch-info lldp neighbors-summary

LLDP neighbor summary.

```
diagnose switch-controller switch-info lldp neighbors-summary <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info lldp stats

LLDP port statistics.

```
diagnose switch-controller switch-info lldp stats <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller switch-info loop-guard

Managed FortiSwitch loop-guard status.

```
diagnose switch-controller switch-info loop-guard <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info mac-limit-violations

Managed FortiSwitch violated MACs.

```
diagnose switch-controller switch-info mac-limit-violations
```

diagnose switch-controller switch-info mac-limit-violations all

FortiSwitch all violations.

```
diagnose switch-controller switch-info mac-limit-violations all <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info mac-limit-violations interface

FortiSwitch port specific violations.

```
diagnose switch-controller switch-info mac-limit-violations interface <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port.	string	

diagnose switch-controller switch-info mac-limit-violations vlan

FortiSwitch VLAN specific violations.

```
diagnose switch-controller switch-info mac-limit-violations vlan <switch> <vlan-id>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<vlan-id>	Managed FortiSwitch VLAN ID.	string	

diagnose switch-controller switch-info mac-table

Managed FortiSwitch MAC address list.

```
diagnose switch-controller switch-info mac-table <switch> <vlan-id>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<vlan-id>	Managed FortiSwitch VLAN of interest for MAC address list.	string	

diagnose switch-controller switch-info mclag

Dumps MCLAG related information from FortiSwitch.

```
diagnose switch-controller switch-info mclag
```

diagnose switch-controller switch-info mclag icl

Dumps MCLAG inter-chassis-link(ICL).

```
diagnose switch-controller switch-info mclag icl <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info mclag list

Dumps MCLAG list.

```
diagnose switch-controller switch-info mclag list <switch> <mclag-trunk-name>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<mclag-trunk-name>	MCLAG's trunk name.	string	

diagnose switch-controller switch-info mclag peer-consistency-check

Checks MCLAG peer consistency.

```
diagnose switch-controller switch-info mclag peer-consistency-check <switch> <mclag-trunk-name>
```


Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<mclag-trunk-name>	MCLAG's trunk name.	string	

diagnose switch-controller switch-info mirror

Managed FortiSwitch mirror information.

```
diagnose switch-controller switch-info mirror
```

diagnose switch-controller switch-info mirror status

Mirror session status.

```
diagnose switch-controller switch-info mirror status <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info modules

Dumps modules related information from FortiSwitch.

```
diagnose switch-controller switch-info modules
```

diagnose switch-controller switch-info modules detail

Managed FortiSwitch module details.

```
diagnose switch-controller switch-info modules detail <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for statistics.	string	

diagnose switch-controller switch-info modules limits

Managed FortiSwitch module limits.

```
diagnose switch-controller switch-info modules limits <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for statistics.	string	

diagnose switch-controller switch-info modules status

Managed FortiSwitch module status.

```
diagnose switch-controller switch-info modules status <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for statistics.	string	

diagnose switch-controller switch-info modules summary

Managed FortiSwitch module summary.

```
diagnose switch-controller switch-info modules summary <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for statistics.	string	

diagnose switch-controller switch-info option82-mapping

Managed FortiSwitch DHCP option 82 mapping.

```
diagnose switch-controller switch-info option82-mapping
```

diagnose switch-controller switch-info option82-mapping snooping

Show DHCP option 82 mapping for snooping configuration.

```
diagnose switch-controller switch-info option82-mapping snooping
```

diagnose switch-controller switch-info option82-mapping snooping ascii

Display DHCP option 82 string in ascii format.

```
diagnose switch-controller switch-info option82-mapping snooping ascii <switch> <vlan> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<vlan>	Managed FortiSwitch VLAN.	string	
<port>	Managed FortiSwitch interface.	string	

diagnose switch-controller switch-info option82-mapping snooping hex

Display DHCP option 82 string in hex format.

```
diagnose switch-controller switch-info option82-mapping snooping hex <switch> <vlan> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<vlan>	Managed FortiSwitch VLAN.	string	
<port>	Managed FortiSwitch interface.	string	

diagnose switch-controller switch-info pdu-counters-list

Managed FortiSwitch pdu-counters.

```
diagnose switch-controller switch-info pdu-counters-list <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info poe

PoE-related information.

```
diagnose switch-controller switch-info poe
```

diagnose switch-controller switch-info poe detail

PoE detail.

```
diagnose switch-controller switch-info poe detail <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller switch-info poe summary

PoE summary.

```
diagnose switch-controller switch-info poe summary <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info port-properties

Managed FortiSwitch port properties.

```
diagnose switch-controller switch-info port-properties <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller switch-info port-stats

Managed FortiSwitch port statistics.

```
diagnose switch-controller switch-info port-stats <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for statistics.	string	

diagnose switch-controller switch-info qos-stats

Managed FortiSwitch QoS statistics.

```
diagnose switch-controller switch-info qos-stats <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for statistics.	string	

diagnose switch-controller switch-info rpvt

Managed FortiSwitch STP port information are inter-operating with rapid PVST network.

```
diagnose switch-controller switch-info rpvt <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller switch-info status

System status.

```
diagnose switch-controller switch-info status <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info stp

Managed FortiSwitch STP instance status.

```
diagnose switch-controller switch-info stp <switch> <instance-id>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<instance-id>	Managed FortiSwitch STP instance of interest for statistics.	string	

diagnose switch-controller switch-info trunk

Trunk information.

```
diagnose switch-controller switch-info trunk
```

diagnose switch-controller switch-info trunk config

Managed FortiSwitch trunk config information.

```
diagnose switch-controller switch-info trunk config <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-info trunk status

Managed FortiSwitch trunk status.

```
diagnose switch-controller switch-info trunk status <switch> <trunk-port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<trunk-port>	Managed FortiSwitch trunk-port of interest for state.	string	

diagnose switch-controller switch-recommendation

Recommendations for FortiLink topology and configuration.

```
diagnose switch-controller switch-recommendation
```

diagnose switch-controller switch-recommendation bios-compatibility-check

FortiSwitch BIOS compatibility check.

```
diagnose switch-controller switch-recommendation bios-compatibility-check <fortilink interface> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-recommendation check-fortilink-link-redundancy

Check if FortiLink trunk has redundant links.

```
diagnose switch-controller switch-recommendation check-fortilink-link-redundancy <fortilink interface> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-recommendation check-isl-icl-link-redundancy

Check if ISL/ICL trunk has redundant links.

```
diagnose switch-controller switch-recommendation check-isl-icl-link-redundancy <fortilink interface> <switch> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch #1 device ID.	string	
<switch>	Managed FortiSwitch #2 device ID.	string	

diagnose switch-controller switch-recommendation check-isl-link-redundancy

Check if ISL trunk has redundant links.

```
diagnose switch-controller switch-recommendation check-isl-link-redundancy <fortilink interface> <switch> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch #1 device ID.	string	
<switch>	Managed FortiSwitch #2 device ID.	string	

diagnose switch-controller switch-recommendation clear-dhcp-opt43-key

Clear DHCP option43 key in topology.

```
diagnose switch-controller switch-recommendation clear-dhcp-opt43-key <fortilink interface>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

diagnose switch-controller switch-recommendation config-dhcp-opt43-key

Config DHCP option43 key in topology.

```
diagnose switch-controller switch-recommendation config-dhcp-opt43-key <fortilink interface> <option 43 key>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<option 43 key>	DHCP option 43 key.	string	

diagnose switch-controller switch-recommendation disable-auto-config-poe-status

Disable PoE status of auto-config default policy.

```
diagnose switch-controller switch-recommendation disable-auto-config-poe-status
```

diagnose switch-controller switch-recommendation disable-bounce-quarantine-link

Disable bounce quarantine link.

```
diagnose switch-controller switch-recommendation disable-bounce-quarantine-link
```

diagnose switch-controller switch-recommendation disable-poe-pre-standard-detection

Disable PoE pre-standard detection for all user ports.

```
diagnose switch-controller switch-recommendation disable-poe-pre-standard-detection <fortilink interface> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-recommendation disable-stp-state-topology

Disable STP state for all user ports.

```
diagnose switch-controller switch-recommendation disable-stp-state-topology <fortilink interface> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-recommendation enable-auto-config-poe-status

Enable PoE status of auto-config default policy.

```
diagnose switch-controller switch-recommendation enable-auto-config-poe-status
```

diagnose switch-controller switch-recommendation enable-bounce-quarantine-link

Enable bounce quarantine link.

```
diagnose switch-controller switch-recommendation enable-bounce-quarantine-link
```

diagnose switch-controller switch-recommendation enable-poe-pre-standard-detection

Enable PoE pre-standard detection for all user ports.

```
diagnose switch-controller switch-recommendation enable-poe-pre-standard-detection <fortilink interface> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-recommendation enable-stp-state-topology

Enable STP state for all user ports.

```
diagnose switch-controller switch-recommendation enable-stp-state-topology <fortilink interface> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-recommendation fabric-lockdown-check

Get fabric lockdown status.

```
diagnose switch-controller switch-recommendation fabric-lockdown-check <fortilink interface>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

diagnose switch-controller switch-recommendation fabric-lockdown-disable

Disable fabric lockdown.

```
diagnose switch-controller switch-recommendation fabric-lockdown-disable <fortilink interface>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

diagnose switch-controller switch-recommendation fabric-lockdown-enable

Enable fabric lockdown.

```
diagnose switch-controller switch-recommendation fabric-lockdown-enable <fortilink interface>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

diagnose switch-controller switch-recommendation get-mclag-tier1-candidate

Get MCLAG tier1 candidate recommendation.

```
diagnose switch-controller switch-recommendation get-mclag-tier1-candidate <fortilink interface>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

diagnose switch-controller switch-recommendation get-mclag-tier2-candidate

Get MCLAG tier2 candidate recommendation.

```
diagnose switch-controller switch-recommendation get-mclag-tier2-candidate <fortilink interface>  
<switch> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID for tier-1 MCLAG peer 1.	string	
<switch>	FortiSwitch device ID for tier-1 MCLAG peer 2.	string	

diagnose switch-controller switch-recommendation get-mclag-tier3-candidate

Get MCLAG tier3 candidate recommendation.

```
diagnose switch-controller switch-recommendation get-mclag-tier3-candidate <fortilink interface>  
<switch> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	FortiSwitch device ID for tier-2 MCLAG peer 1.	string	
<switch>	FortiSwitch device ID for tier-2 MCLAG peer 2.	string	

diagnose switch-controller switch-recommendation is-fortilink-capacity-exceeded

Check if FortiLink is almost at capacity.

```
diagnose switch-controller switch-recommendation is-fortilink-capacity-exceeded
```

diagnose switch-controller switch-recommendation is-switch-dual-homed

Check if switch is dual-homed.

```
diagnose switch-controller switch-recommendation is-switch-dual-homed <fortilink interface>  
<switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-recommendation lock-down-topo-lldp-profile

Lock down topology via LLDP profile.

```
diagnose switch-controller switch-recommendation lock-down-topo-lldp-profile <fortilink interface> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller switch-recommendation pse-check

Get fabric PSE-PSE status.

```
diagnose switch-controller switch-recommendation pse-check <fortilink interface>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

diagnose switch-controller switch-recommendation pse-config

Disable fabric POE-status to prevent PSE-PSE scenarios.

```
diagnose switch-controller switch-recommendation pse-config <fortilink interface>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

diagnose switch-controller switch-recommendation set-tier-plus-mclag-icl

Configure tier-plus MCLAG-ICL.

```
diagnose switch-controller switch-recommendation set-tier-plus-mclag-icl <fortilink interface>
<switch> <switch> <switch> <switch> <isl-port-group-name>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	FortiSwitch device ID for parent MCLAG peer 1.	string	
<switch>	FortiSwitch device ID for parent MCLAG peer 2.	string	
<switch>	FortiSwitch device ID for child MCLAG peer 1.	string	
<switch>	FortiSwitch device ID for child MCLAG peer 2.	string	
<isl-port-group-name>	Unique ISL port group name.	string	

diagnose switch-controller switch-recommendation set-tier1-mclag-icl

Configure tier-1 MCLAG-ICL.

```
diagnose switch-controller switch-recommendation set-tier1-mclag-icl <fortilink interface>
<switch> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	FortiSwitch device ID for MCLAG peer 1.	string	
<switch>	FortiSwitch device ID for MCLAG peer 2.	string	

diagnose switch-controller switch-recommendation tunnel-mode-settings

Tunnel mode settings.

```
diagnose switch-controller switch-recommendation tunnel-mode-settings <fortilink interface>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	

diagnose switch-controller switch-recommendation unlock-topo-lldp-profile

Unlock topology via LLDP profile.

```
diagnose switch-controller switch-recommendation unlock-topo-lldp-profile <fortilink interface> <switch>
```

Parameter	Description	Type	Size
<fortilink interface>	FortiLink interface name.	string	
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller system-info

Switch-controller system information.

```
diagnose switch-controller system-info
```

diagnose switch-controller system-info show

Show switch-controller system info.

```
diagnose switch-controller system-info show
```

diagnose switch-controller telemetry

FortiSwitch telemetry.

```
diagnose switch-controller telemetry
```

diagnose switch-controller telemetry show

Show FortiSwitch telemetry.


```
diagnose switch-controller telemetry show
```

diagnose switch-controller telemetry show mac-stats

Show FortiSwitch MAC telemetry.

```
diagnose switch-controller telemetry show mac-stats
```

diagnose switch-controller telemetry show mac-stats switch

Show FortiSwitch telemetry.

```
diagnose switch-controller telemetry show mac-stats switch <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller telemetry show switch

Show FortiSwitch telemetry.

```
diagnose switch-controller telemetry show switch <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller telemetry show switch-port

Show FortiSwitch port telemetry.

```
diagnose switch-controller telemetry show switch-port <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port of interest for telemetry.	string	

diagnose switch-controller topology

Topology commands.

```
diagnose switch-controller topology
```

diagnose switch-controller topology reset

Topology reset commands.

```
diagnose switch-controller topology reset
```

diagnose switch-controller topology reset fortilink-flag

Reset FortiLink flag.

```
diagnose switch-controller topology reset fortilink-flag <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller topology reset isl-peer-flag

Reset isl peer flag.

```
diagnose switch-controller topology reset isl-peer-flag <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller topology set

Topology set commands.

```
diagnose switch-controller topology set
```

diagnose switch-controller topology set fortilink-flag

Set FortiLink flag.

```
diagnose switch-controller topology set fortilink-flag <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller topology set isl-peer-flag

Set isl peer flag.

```
diagnose switch-controller topology set isl-peer-flag <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port name.	string	

diagnose switch-controller traffic-capture

Traffic capture.

```
diagnose switch-controller traffic-capture
```

diagnose switch-controller traffic-capture show

Dump all sniffer sessions.

```
diagnose switch-controller traffic-capture show
```

diagnose switch-controller traffic-capture start

Start sniffer session.

```
diagnose switch-controller traffic-capture start <fortilink-interface> <mac>
```

Parameter	Description	Type	Size
<fortilink-interface>	FortiLink interface name.	string	
<mac>	Device MAC Address.	string	

diagnose switch-controller traffic-capture stop

Stop sniffer session and callback.

```
diagnose switch-controller traffic-capture stop <fortilink-interface> <mac>
```

Parameter	Description	Type	Size
<fortilink-interface>	FortiLink interface name.	string	
<mac>	Device MAC Address.	string	

diagnose switch-controller trigger

Trigger switch controller processing.

```
diagnose switch-controller trigger
```

diagnose switch-controller trigger config-sync

Triggers full configuration synchronization for FortiSwitch.

```
diagnose switch-controller trigger config-sync <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller trigger mac-sync

Trigger MAC sync for all managed FortiSwitches.

```
diagnose switch-controller trigger mac-sync
```

diagnose switch-controller trigger nac-mac-cache-sync

Triggers NAC MAC cache synchronization from FortiSwitch.

```
diagnose switch-controller trigger nac-mac-cache-sync <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose switch-controller trigger reset-hardware-counters

Triggers reset of port statistic counters for FortiSwitch.

```
diagnose switch-controller trigger reset-hardware-counters <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port list (range of ports separated by commas; eg 1,3,1-4,port6-7,port10-port11,internal).	string	

diagnose switch-controller trigger restore-hardware-counters

Triggers restoration of port statistic counters from FortiSwitch hardware.

```
diagnose switch-controller trigger restore-hardware-counters <switch> <port>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	
<port>	Managed FortiSwitch port list (range of ports separated by commas; eg 1,3,1-4,port6-7,port10-port11,internal).	string	

diagnose switch-controller tunnel-status

Switch-controller tunnel status.

```
diagnose switch-controller tunnel-status <switch>
```

Parameter	Description	Type	Size
<switch>	Managed FortiSwitch device ID.	string	

diagnose sys

system

This topic includes the following commands:

- [diagnose sys acme on page 3135](#)
- [diagnose sys acme add-account on page 3135](#)
- [diagnose sys acme clear-staging on page 3135](#)
- [diagnose sys acme debug on page 3136](#)
- [diagnose sys acme debug disable on page 3136](#)
- [diagnose sys acme debug enable on page 3136](#)
- [diagnose sys acme debug enable level on page 3136](#)
- [diagnose sys acme debug enable level debug on page 3136](#)
- [diagnose sys acme debug enable level error on page 3136](#)
- [diagnose sys acme debug enable level info on page 3137](#)
- [diagnose sys acme debug enable level verbose on page 3137](#)
- [diagnose sys acme debug enable level veryverbose on page 3137](#)
- [diagnose sys acme debug enable level warning on page 3137](#)
- [diagnose sys acme delete-cert on page 3137](#)
- [diagnose sys acme force-renew on page 3137](#)
- [diagnose sys acme list-archive on page 3138](#)
- [diagnose sys acme list-domains on page 3138](#)
- [diagnose sys acme purge-all on page 3138](#)
- [diagnose sys acme purge-archive on page 3138](#)
- [diagnose sys acme purge-certs on page 3138](#)
- [diagnose sys acme regenerate-client-config on page 3138](#)
- [diagnose sys acme regenerate-store on page 3139](#)
- [diagnose sys acme restart on page 3139](#)
- [diagnose sys acme show-archive on page 3139](#)
- [diagnose sys acme show-client-config on page 3139](#)
- [diagnose sys acme show-passphrase on page 3139](#)
- [diagnose sys acme status-full on page 3139](#)
- [diagnose sys botnet-domain on page 3140](#)
- [diagnose sys botnet-domain hit on page 3140](#)
- [diagnose sys botnet-domain list on page 3140](#)
- [diagnose sys botnet-ip on page 3140](#)
- [diagnose sys botnet-ip find on page 3140](#)

- [diagnose sys botnet-ip flush on page 3141](#)
- [diagnose sys botnet-ip hit on page 3141](#)
- [diagnose sys botnet-ip list on page 3141](#)
- [diagnose sys certificate-blocklist on page 3141](#)
- [diagnose sys certificate-blocklist count on page 3141](#)
- [diagnose sys certificate-blocklist delete-mcddb on page 3142](#)
- [diagnose sys certificate-blocklist query on page 3142](#)
- [diagnose sys certificate-blocklist read-range on page 3142](#)
- [diagnose sys certificate-blocklist status on page 3142](#)
- [diagnose sys cmdb on page 3142](#)
- [diagnose sys cmdb buf-sz on page 3143](#)
- [diagnose sys cmdb dump on page 3143](#)
- [diagnose sys cmdb dump vdom on page 3143](#)
- [diagnose sys cmdb flag on page 3143](#)
- [diagnose sys cmdb flag info on page 3143](#)
- [diagnose sys cmdb flag reset on page 3143](#)
- [diagnose sys cmdb flag reset script-running on page 3144](#)
- [diagnose sys cmdb info on page 3144](#)
- [diagnose sys cmdb obj-verno on page 3144](#)
- [diagnose sys cmdb refcnt on page 3144](#)
- [diagnose sys cmdb refcnt reset on page 3144](#)
- [diagnose sys cmdb refcnt show on page 3145](#)
- [diagnose sys cmdb set-readlock on page 3145](#)
- [diagnose sys cmdb unset-readlock on page 3145](#)
- [diagnose sys cmdb-profile on page 3145](#)
- [diagnose sys cmdb-profile info on page 3145](#)
- [diagnose sys cmdb-profile node on page 3145](#)
- [diagnose sys cmdb-profile reset on page 3146](#)
- [diagnose sys cmdb-profile top10 on page 3146](#)
- [diagnose sys cmdb-profile top10 average on page 3146](#)
- [diagnose sys cmdb-profile top10 total on page 3146](#)
- [diagnose sys config-transaction on page 3146](#)
- [diagnose sys config-transaction show on page 3147](#)
- [diagnose sys config-transaction show entity-by-txn on page 3147](#)
- [diagnose sys config-transaction show mctx on page 3147](#)
- [diagnose sys config-transaction show txn-cli-commands on page 3147](#)
- [diagnose sys config-transaction show txn-entity on page 3147](#)
- [diagnose sys config-transaction show txn-info on page 3148](#)
- [diagnose sys config-transaction show txn-lock on page 3148](#)
- [diagnose sys config-transaction show txn-meta on page 3148](#)
- [diagnose sys config-transaction status on page 3148](#)
- [diagnose sys cpuset on page 3148](#)
- [diagnose sys cpuset interrupt on page 3148](#)

- [diagnose sys cpuset process on page 3149](#)
- [diagnose sys csf on page 3149](#)
- [diagnose sys csf authorization on page 3149](#)
- [diagnose sys csf authorization accept on page 3149](#)
- [diagnose sys csf authorization deny on page 3149](#)
- [diagnose sys csf authorization pending-list on page 3150](#)
- [diagnose sys csf downstream on page 3150](#)
- [diagnose sys csf downstream-devices on page 3150](#)
- [diagnose sys csf dynamic-sync-read on page 3150](#)
- [diagnose sys csf dynamic-sync-request on page 3151](#)
- [diagnose sys csf dynamic-sync-update on page 3151](#)
- [diagnose sys csf fabric-device on page 3151](#)
- [diagnose sys csf fabric-device list on page 3151](#)
- [diagnose sys csf file on page 3151](#)
- [diagnose sys csf file cat on page 3152](#)
- [diagnose sys csf file top-mem on page 3152](#)
- [diagnose sys csf forticloud-id-list on page 3152](#)
- [diagnose sys csf get-bulk-global-view on page 3152](#)
- [diagnose sys csf global on page 3152](#)
- [diagnose sys csf initialize-cmd on page 3153](#)
- [diagnose sys csf merge-cmd on page 3153](#)
- [diagnose sys csf neighbor on page 3153](#)
- [diagnose sys csf neighbor flush on page 3153](#)
- [diagnose sys csf neighbor list on page 3154](#)
- [diagnose sys csf query on page 3154](#)
- [diagnose sys csf ratelimit-test-sender on page 3154](#)
- [diagnose sys csf ratelimit-test-server on page 3154](#)
- [diagnose sys csf send-test-log-upstream on page 3155](#)
- [diagnose sys csf seqpacket-message-listener on page 3155](#)
- [diagnose sys csf seqpacket-message-sender on page 3155](#)
- [diagnose sys csf stream-message-listener on page 3155](#)
- [diagnose sys csf stream-message-sender on page 3156](#)
- [diagnose sys csf trigger-info-update on page 3156](#)
- [diagnose sys csf tunnel-test-listener on page 3156](#)
- [diagnose sys csf tunnel-test-sender on page 3156](#)
- [diagnose sys csf upstream on page 3157](#)
- [diagnose sys csf versions on page 3157](#)
- [diagnose sys csum on page 3157](#)
- [diagnose sys dayst-info on page 3157](#)
- [diagnose sys device on page 3157](#)
- [diagnose sys device add on page 3158](#)
- [diagnose sys device delete on page 3158](#)
- [diagnose sys device list on page 3158](#)

- [diagnose sys dump-conserve-info on page 3158](#)
- [diagnose sys emac-vlan on page 3158](#)
- [diagnose sys emac-vlan fdb on page 3159](#)
- [diagnose sys emac-vlan fdb list on page 3159](#)
- [diagnose sys emac-vlan stat on page 3159](#)
- [diagnose sys external-address-resource on page 3159](#)
- [diagnose sys external-address-resource list on page 3159](#)
- [diagnose sys external-generic-address-resource on page 3160](#)
- [diagnose sys external-generic-address-resource remove-by-name on page 3160](#)
- [diagnose sys external-generic-address-resource remove-by-namespace on page 3160](#)
- [diagnose sys external-mac-resource on page 3160](#)
- [diagnose sys external-mac-resource list on page 3161](#)
- [diagnose sys external-resource on page 3161](#)
- [diagnose sys external-resource list on page 3161](#)
- [diagnose sys external-resource push-add on page 3161](#)
- [diagnose sys external-resource push-api-json-commands on page 3161](#)
- [diagnose sys external-resource push-remove on page 3162](#)
- [diagnose sys external-resource push-snapshot on page 3162](#)
- [diagnose sys external-resource stats on page 3162](#)
- [diagnose sys filesystem on page 3162](#)
- [diagnose sys filesystem hash on page 3162](#)
- [diagnose sys filesystem last-modified-files on page 3162](#)
- [diagnose sys filesystem lsof on page 3163](#)
- [diagnose sys filesystem open-files on page 3163](#)
- [diagnose sys filesystem tree on page 3163](#)
- [diagnose sys fips on page 3163](#)
- [diagnose sys fips error-mode on page 3164](#)
- [diagnose sys fips kat-error on page 3164](#)
- [diagnose sys flash on page 3164](#)
- [diagnose sys flash format on page 3164](#)
- [diagnose sys flash list on page 3164](#)
- [diagnose sys forticonverter on page 3165](#)
- [diagnose sys forticonverter available-source-devices on page 3165](#)
- [diagnose sys forticonverter create-ticket on page 3165](#)
- [diagnose sys forticonverter custom-create-ticket on page 3165](#)
- [diagnose sys forticonverter download-status on page 3165](#)
- [diagnose sys forticonverter eligibility-status on page 3166](#)
- [diagnose sys forticonverter get-prompt-visibility on page 3166](#)
- [diagnose sys forticonverter result-availability on page 3166](#)
- [diagnose sys forticonverter set-source-fortigate on page 3166](#)
- [diagnose sys forticonverter source-config-upload-status on page 3167](#)
- [diagnose sys forticonverter source-interfaces on page 3167](#)
- [diagnose sys forticonverter start-download on page 3167](#)

- [diagnose sys forticonverter submitted-info on page 3167](#)
- [diagnose sys forticonverter update-eligibility on page 3168](#)
- [diagnose sys forticonverter update-result-availability on page 3168](#)
- [diagnose sys forticonverter upload-local-config on page 3168](#)
- [diagnose sys forticonverter upload-status on page 3168](#)
- [diagnose sys frag-mem on page 3168](#)
- [diagnose sys fullcone on page 3169](#)
- [diagnose sys geneve on page 3169](#)
- [diagnose sys geneve list on page 3169](#)
- [diagnose sys geneve stat on page 3169](#)
- [diagnose sys gre on page 3169](#)
- [diagnose sys gre keepalive on page 3169](#)
- [diagnose sys gre list on page 3170](#)
- [diagnose sys h323 on page 3170](#)
- [diagnose sys h323 call on page 3170](#)
- [diagnose sys h323 call list on page 3170](#)
- [diagnose sys h323 debug-mask on page 3170](#)
- [diagnose sys h323 peer on page 3170](#)
- [diagnose sys h323 peer list on page 3171](#)
- [diagnose sys h323 status on page 3171](#)
- [diagnose sys ha on page 3171](#)
- [diagnose sys ha autoscale-peers on page 3171](#)
- [diagnose sys ha check-vc on page 3171](#)
- [diagnose sys ha checksum on page 3171](#)
- [diagnose sys ha checksum autoscale-cluster on page 3172](#)
- [diagnose sys ha checksum cached on page 3172](#)
- [diagnose sys ha checksum cluster on page 3172](#)
- [diagnose sys ha checksum log on page 3172](#)
- [diagnose sys ha checksum log clear on page 3172](#)
- [diagnose sys ha checksum log disable on page 3173](#)
- [diagnose sys ha checksum log enable on page 3173](#)
- [diagnose sys ha checksum recalculate on page 3173](#)
- [diagnose sys ha checksum show on page 3173](#)
- [diagnose sys ha checksum show-nonsync on page 3174](#)
- [diagnose sys ha checksum test on page 3174](#)
- [diagnose sys ha dump-by on page 3174](#)
- [diagnose sys ha dump-by debug-zone on page 3174](#)
- [diagnose sys ha dump-by device on page 3174](#)
- [diagnose sys ha dump-by group on page 3174](#)
- [diagnose sys ha dump-by kernel on page 3175](#)
- [diagnose sys ha dump-by rcache on page 3175](#)
- [diagnose sys ha dump-by vcluster on page 3175](#)
- [diagnose sys ha dump-by vdom on page 3175](#)

- [diagnose sys ha extfile-sig on page 3175](#)
- [diagnose sys ha fgsp-zone on page 3175](#)
- [diagnose sys ha fib on page 3176](#)
- [diagnose sys ha hactx-stats on page 3176](#)
- [diagnose sys ha hactx-stats clear on page 3176](#)
- [diagnose sys ha hadiff on page 3176](#)
- [diagnose sys ha hadiff log on page 3176](#)
- [diagnose sys ha hadiff log clear on page 3176](#)
- [diagnose sys ha hadiff log disable on page 3177](#)
- [diagnose sys ha hadiff log enable on page 3177](#)
- [diagnose sys ha hadiff max-sync-turns on page 3177](#)
- [diagnose sys ha hadiff max-unsync-wait on page 3177](#)
- [diagnose sys ha hadiff status on page 3177](#)
- [diagnose sys ha hadiff sync-from-higher on page 3178](#)
- [diagnose sys ha hasync-conn-max-buf on page 3178](#)
- [diagnose sys ha hasync-stats on page 3178](#)
- [diagnose sys ha hasync-stats all on page 3178](#)
- [diagnose sys ha hasync-stats by-object on page 3178](#)
- [diagnose sys ha hasync-stats most-recent on page 3179](#)
- [diagnose sys ha hasync-stats most-time on page 3179](#)
- [diagnose sys ha heartbeat on page 3179](#)
- [diagnose sys ha history on page 3179](#)
- [diagnose sys ha history clear on page 3179](#)
- [diagnose sys ha history read on page 3180](#)
- [diagnose sys ha mac on page 3180](#)
- [diagnose sys ha pingsvr-secondary-force-reset on page 3180](#)
- [diagnose sys ha recalculate-extfile-signature on page 3180](#)
- [diagnose sys ha reset-health-status on page 3180](#)
- [diagnose sys ha reset-uptime on page 3180](#)
- [diagnose sys ha reset-uptime-primary-only on page 3181](#)
- [diagnose sys ha session-sync-dev on page 3181](#)
- [diagnose sys ha session-sync-dev clear on page 3181](#)
- [diagnose sys ha session-sync-dev set on page 3181](#)
- [diagnose sys ha standalone-peers on page 3181](#)
- [diagnose sys ha standalone-peers reset-stats on page 3181](#)
- [diagnose sys ha stats on page 3182](#)
- [diagnose sys ha status on page 3182](#)
- [diagnose sys ha sync-stats on page 3182](#)
- [diagnose sys ha sync-stats-reset on page 3182](#)
- [diagnose sys ha vlan-hb-monitor on page 3182](#)
- [diagnose sys icap-remote-server on page 3182](#)
- [diagnose sys icap-remote-server status on page 3183](#)
- [diagnose sys icb on page 3183](#)

- [diagnose sys icb debug on page 3183](#)
- [diagnose sys icb debug disable on page 3183](#)
- [diagnose sys icb debug info on page 3183](#)
- [diagnose sys icb debug show on page 3183](#)
- [diagnose sys icb debug verbose on page 3184](#)
- [diagnose sys icb stats on page 3184](#)
- [diagnose sys icb stats list on page 3184](#)
- [diagnose sys icb status on page 3184](#)
- [diagnose sys icb status current on page 3184](#)
- [diagnose sys iotop on page 3184](#)
- [diagnose sys ipam on page 3185](#)
- [diagnose sys ipam delete on page 3185](#)
- [diagnose sys ipam delete device on page 3185](#)
- [diagnose sys ipam largest-available-subnet on page 3185](#)
- [diagnose sys ipam list on page 3185](#)
- [diagnose sys ipam list entries on page 3185](#)
- [diagnose sys ipam list free-subnets on page 3186](#)
- [diagnose sys ipsec-aggregate on page 3186](#)
- [diagnose sys ipsec-aggregate list on page 3186](#)
- [diagnose sys kill on page 3186](#)
- [diagnose sys link-monitor on page 3186](#)
- [diagnose sys link-monitor filter on page 3187](#)
- [diagnose sys link-monitor filter clear on page 3187](#)
- [diagnose sys link-monitor filter name on page 3187](#)
- [diagnose sys link-monitor interface on page 3187](#)
- [diagnose sys link-monitor launch on page 3187](#)
- [diagnose sys link-monitor reset-monitor on page 3188](#)
- [diagnose sys link-monitor sdwan-hc on page 3188](#)
- [diagnose sys link-monitor sdwan-service on page 3188](#)
- [diagnose sys link-monitor shm-band-stats on page 3188](#)
- [diagnose sys link-monitor shm-stats on page 3189](#)
- [diagnose sys link-monitor status on page 3189](#)
- [diagnose sys link-monitor tunnel on page 3189](#)
- [diagnose sys link-monitor zone-intf on page 3189](#)
- [diagnose sys link-monitor-passive on page 3190](#)
- [diagnose sys link-monitor-passive admin on page 3190](#)
- [diagnose sys link-monitor-passive admin dbg-rpt on page 3190](#)
- [diagnose sys link-monitor-passive admin dbg-rpt reset on page 3190](#)
- [diagnose sys link-monitor-passive admin dbg-rpt retrans on page 3190](#)
- [diagnose sys link-monitor-passive admin dbg-rpt rtt on page 3191](#)
- [diagnose sys link-monitor-passive admin dbg-rpt syn-retrans on page 3191](#)
- [diagnose sys link-monitor-passive admin delete on page 3192](#)
- [diagnose sys link-monitor-passive admin flush on page 3192](#)

- [diagnose sys link-monitor-passive admin list on page 3192](#)
- [diagnose sys link-monitor-passive admin list by-application on page 3193](#)
- [diagnose sys link-monitor-passive admin list by-interface on page 3193](#)
- [diagnose sys link-monitor-passive agent on page 3193](#)
- [diagnose sys link-monitor-passive agent agent-oif-map on page 3193](#)
- [diagnose sys link-monitor-passive agent flush on page 3193](#)
- [diagnose sys link-monitor-passive agent flush-app on page 3194](#)
- [diagnose sys link-monitor-passive agent list on page 3194](#)
- [diagnose sys link-monitor-passive agent list-app on page 3194](#)
- [diagnose sys link-monitor-passive agent send-report on page 3194](#)
- [diagnose sys link-monitor-passive remote on page 3195](#)
- [diagnose sys link-monitor-passive remote list on page 3195](#)
- [diagnose sys logdisk on page 3195](#)
- [diagnose sys logdisk purge-log-data on page 3195](#)
- [diagnose sys logdisk quota on page 3195](#)
- [diagnose sys logdisk smart on page 3195](#)
- [diagnose sys logdisk status on page 3196](#)
- [diagnose sys logdisk status monitor on page 3196](#)
- [diagnose sys logdisk usage on page 3196](#)
- [diagnose sys mcast-session on page 3196](#)
- [diagnose sys mcast-session clear on page 3196](#)
- [diagnose sys mcast-session filter on page 3196](#)
- [diagnose sys mcast-session filter clear on page 3197](#)
- [diagnose sys mcast-session filter clear dport on page 3197](#)
- [diagnose sys mcast-session filter clear dst on page 3197](#)
- [diagnose sys mcast-session filter clear proto on page 3197](#)
- [diagnose sys mcast-session filter clear sintf on page 3197](#)
- [diagnose sys mcast-session filter clear sport on page 3197](#)
- [diagnose sys mcast-session filter clear src on page 3198](#)
- [diagnose sys mcast-session filter clear vd on page 3198](#)
- [diagnose sys mcast-session filter dport on page 3198](#)
- [diagnose sys mcast-session filter dst on page 3198](#)
- [diagnose sys mcast-session filter negate on page 3198](#)
- [diagnose sys mcast-session filter negate dport on page 3199](#)
- [diagnose sys mcast-session filter negate dst on page 3199](#)
- [diagnose sys mcast-session filter negate proto on page 3199](#)
- [diagnose sys mcast-session filter negate sintf on page 3199](#)
- [diagnose sys mcast-session filter negate sport on page 3199](#)
- [diagnose sys mcast-session filter negate src on page 3199](#)
- [diagnose sys mcast-session filter negate vd on page 3200](#)
- [diagnose sys mcast-session filter proto on page 3200](#)
- [diagnose sys mcast-session filter sintf on page 3200](#)
- [diagnose sys mcast-session filter sport on page 3200](#)

- [diagnose sys mcast-session filter src on page 3200](#)
- [diagnose sys mcast-session filter vd on page 3201](#)
- [diagnose sys mcast-session list on page 3201](#)
- [diagnose sys mcast-session stat on page 3201](#)
- [diagnose sys mcast-session6 on page 3201](#)
- [diagnose sys mcast-session6 clear on page 3201](#)
- [diagnose sys mcast-session6 filter on page 3202](#)
- [diagnose sys mcast-session6 filter clear on page 3202](#)
- [diagnose sys mcast-session6 filter clear dport on page 3202](#)
- [diagnose sys mcast-session6 filter clear dst on page 3202](#)
- [diagnose sys mcast-session6 filter clear proto on page 3202](#)
- [diagnose sys mcast-session6 filter clear sintf on page 3202](#)
- [diagnose sys mcast-session6 filter clear sport on page 3203](#)
- [diagnose sys mcast-session6 filter clear src on page 3203](#)
- [diagnose sys mcast-session6 filter clear vd on page 3203](#)
- [diagnose sys mcast-session6 filter dport on page 3203](#)
- [diagnose sys mcast-session6 filter dst on page 3203](#)
- [diagnose sys mcast-session6 filter negate on page 3204](#)
- [diagnose sys mcast-session6 filter negate dport on page 3204](#)
- [diagnose sys mcast-session6 filter negate dst on page 3204](#)
- [diagnose sys mcast-session6 filter negate proto on page 3204](#)
- [diagnose sys mcast-session6 filter negate sintf on page 3204](#)
- [diagnose sys mcast-session6 filter negate sport on page 3204](#)
- [diagnose sys mcast-session6 filter negate src on page 3205](#)
- [diagnose sys mcast-session6 filter negate vd on page 3205](#)
- [diagnose sys mcast-session6 filter proto on page 3205](#)
- [diagnose sys mcast-session6 filter sintf on page 3205](#)
- [diagnose sys mcast-session6 filter sport on page 3205](#)
- [diagnose sys mcast-session6 filter src on page 3206](#)
- [diagnose sys mcast-session6 filter vd on page 3206](#)
- [diagnose sys mcast-session6 list on page 3206](#)
- [diagnose sys mcast-session6 stat on page 3206](#)
- [diagnose sys mpstat on page 3207](#)
- [diagnose sys ntp on page 3207](#)
- [diagnose sys ntp status on page 3207](#)
- [diagnose sys pair on page 3207](#)
- [diagnose sys platform on page 3207](#)
- [diagnose sys platform info on page 3207](#)
- [diagnose sys print-conserve-info on page 3208](#)
- [diagnose sys process on page 3208](#)
- [diagnose sys process daemon-auto-restart on page 3208](#)
- [diagnose sys process dump on page 3208](#)
- [diagnose sys process nameof on page 3208](#)

- [diagnose sys process pidof on page 3209](#)
- [diagnose sys process pstack on page 3209](#)
- [diagnose sys process sock-mem on page 3209](#)
- [diagnose sys process socket on page 3209](#)
- [diagnose sys process trace on page 3209](#)
- [diagnose sys profile on page 3210](#)
- [diagnose sys profile cpumask on page 3210](#)
- [diagnose sys profile module on page 3210](#)
- [diagnose sys profile show on page 3210](#)
- [diagnose sys profile show detail on page 3210](#)
- [diagnose sys profile show order on page 3210](#)
- [diagnose sys profile start on page 3211](#)
- [diagnose sys profile step on page 3211](#)
- [diagnose sys profile stop on page 3211](#)
- [diagnose sys profile sysmap on page 3211](#)
- [diagnose sys proxy on page 3211](#)
- [diagnose sys proxy bypass on page 3211](#)
- [diagnose sys proxy bypass clear on page 3212](#)
- [diagnose sys proxy bypass disable on page 3212](#)
- [diagnose sys proxy bypass disable category on page 3212](#)
- [diagnose sys proxy bypass disable category all on page 3212](#)
- [diagnose sys proxy bypass disable category scanunit-submission on page 3212](#)
- [diagnose sys proxy bypass disable category ssl on page 3212](#)
- [diagnose sys proxy bypass disable category utm on page 3213](#)
- [diagnose sys proxy bypass disable protocol on page 3213](#)
- [diagnose sys proxy bypass disable protocol all on page 3213](#)
- [diagnose sys proxy bypass disable protocol ftp on page 3213](#)
- [diagnose sys proxy bypass disable protocol imap on page 3213](#)
- [diagnose sys proxy bypass disable protocol nntp on page 3213](#)
- [diagnose sys proxy bypass disable protocol pop3 on page 3214](#)
- [diagnose sys proxy bypass disable protocol smtp on page 3214](#)
- [diagnose sys proxy bypass enable on page 3214](#)
- [diagnose sys proxy bypass enable category on page 3214](#)
- [diagnose sys proxy bypass enable category all on page 3214](#)
- [diagnose sys proxy bypass enable category scanunit-submission on page 3214](#)
- [diagnose sys proxy bypass enable category ssl on page 3215](#)
- [diagnose sys proxy bypass enable category utm on page 3215](#)
- [diagnose sys proxy bypass enable protocol on page 3215](#)
- [diagnose sys proxy bypass enable protocol all on page 3215](#)
- [diagnose sys proxy bypass enable protocol ftp on page 3215](#)
- [diagnose sys proxy bypass enable protocol imap on page 3215](#)
- [diagnose sys proxy bypass enable protocol nntp on page 3216](#)
- [diagnose sys proxy bypass enable protocol pop3 on page 3216](#)

- [diagnose sys proxy bypass enable protocol smtp on page 3216](#)
- [diagnose sys proxy bypass show on page 3216](#)
- [diagnose sys proxy certificate-blocklist on page 3216](#)
- [diagnose sys proxy certificate-blocklist flush on page 3216](#)
- [diagnose sys proxy certificate-blocklist status on page 3217](#)
- [diagnose sys proxy debug-filter on page 3217](#)
- [diagnose sys proxy debug-filter clear on page 3217](#)
- [diagnose sys proxy debug-filter list on page 3217](#)
- [diagnose sys proxy debug-filter src on page 3217](#)
- [diagnose sys proxy filter on page 3217](#)
- [diagnose sys proxy filter clear on page 3218](#)
- [diagnose sys proxy filter list on page 3218](#)
- [diagnose sys proxy filter negate on page 3218](#)
- [diagnose sys proxy filter negate vd on page 3218](#)
- [diagnose sys proxy filter negate worker on page 3218](#)
- [diagnose sys proxy filter vd on page 3218](#)
- [diagnose sys proxy filter worker on page 3219](#)
- [diagnose sys proxy log on page 3219](#)
- [diagnose sys proxy log filter on page 3219](#)
- [diagnose sys proxy log filter clear on page 3219](#)
- [diagnose sys proxy log filter list on page 3219](#)
- [diagnose sys proxy log filter negate on page 3219](#)
- [diagnose sys proxy log filter negate vd on page 3220](#)
- [diagnose sys proxy log filter negate worker on page 3220](#)
- [diagnose sys proxy log filter vd on page 3220](#)
- [diagnose sys proxy log filter worker on page 3220](#)
- [diagnose sys proxy log-debug on page 3220](#)
- [diagnose sys proxy memory on page 3221](#)
- [diagnose sys proxy memory allocator on page 3221](#)
- [diagnose sys proxy memory conserve on page 3221](#)
- [diagnose sys proxy memory conserve enter on page 3221](#)
- [diagnose sys proxy memory conserve exit on page 3221](#)
- [diagnose sys proxy memory jemalloc on page 3221](#)
- [diagnose sys proxy memory malloc on page 3222](#)
- [diagnose sys proxy memory usage on page 3222](#)
- [diagnose sys proxy restart on page 3222](#)
- [diagnose sys proxy simulate-error on page 3222](#)
- [diagnose sys proxy simulate-error scan-drop on page 3222](#)
- [diagnose sys proxy simulate-error scan-drop disable on page 3222](#)
- [diagnose sys proxy simulate-error scan-drop enable on page 3223](#)
- [diagnose sys proxy simulate-error status on page 3223](#)
- [diagnose sys proxy socket-options on page 3223](#)
- [diagnose sys proxy socket-options linger on page 3223](#)

- [diagnose sys proxy socket-options linger disable on page 3223](#)
- [diagnose sys proxy socket-options linger enable on page 3223](#)
- [diagnose sys proxy socket-options nagle on page 3224](#)
- [diagnose sys proxy socket-options nagle disable on page 3224](#)
- [diagnose sys proxy socket-options nagle enable on page 3224](#)
- [diagnose sys proxy socket-options status on page 3224](#)
- [diagnose sys proxy ssl on page 3224](#)
- [diagnose sys proxy ssl bypass on page 3224](#)
- [diagnose sys proxy ssl bypass flush on page 3225](#)
- [diagnose sys proxy ssl bypass list on page 3225](#)
- [diagnose sys proxy ssl crypto on page 3225](#)
- [diagnose sys proxy ssl crypto async on page 3225](#)
- [diagnose sys proxy ssl crypto sync on page 3225](#)
- [diagnose sys proxy ssl exempt on page 3225](#)
- [diagnose sys proxy ssl exempt flush on page 3226](#)
- [diagnose sys proxy ssl exempt list on page 3226](#)
- [diagnose sys proxy ssl rsa-blinding on page 3226](#)
- [diagnose sys proxy ssl rsa-blinding off on page 3226](#)
- [diagnose sys proxy ssl rsa-blinding on on page 3226](#)
- [diagnose sys proxy ssl session on page 3226](#)
- [diagnose sys proxy stats on page 3227](#)
- [diagnose sys proxy stats all on page 3227](#)
- [diagnose sys proxy stats clear on page 3227](#)
- [diagnose sys proxy stats debug on page 3227](#)
- [diagnose sys proxy stats list on page 3227](#)
- [diagnose sys proxy stats protocol on page 3227](#)
- [diagnose sys proxy stats vdom on page 3228](#)
- [diagnose sys proxy stats vdom all on page 3228](#)
- [diagnose sys proxy stats vdom list on page 3228](#)
- [diagnose sys proxy stats vdom summary on page 3228](#)
- [diagnose sys proxy valgrind on page 3228](#)
- [diagnose sys proxy valgrind disable on page 3228](#)
- [diagnose sys proxy valgrind enable on page 3229](#)
- [diagnose sys proxy valgrind log on page 3229](#)
- [diagnose sys proxy valgrind log clear on page 3229](#)
- [diagnose sys proxy valgrind log show on page 3229](#)
- [diagnose sys proxy valgrind memcheck on page 3229](#)
- [diagnose sys proxy valgrind memcheck_less on page 3229](#)
- [diagnose sys proxy valgrind status on page 3230](#)
- [diagnose sys ptp on page 3230](#)
- [diagnose sys ptp status on page 3230](#)
- [diagnose sys route_tag on page 3230](#)
- [diagnose sys route_tag flush on page 3230](#)

- [diagnose sys route_tag list on page 3230](#)
- [diagnose sys route_tag summary on page 3231](#)
- [diagnose sys saml on page 3231](#)
- [diagnose sys saml metadata on page 3231](#)
- [diagnose sys scanunit on page 3231](#)
- [diagnose sys scanunit auto-restart on page 3231](#)
- [diagnose sys scanunit auto-restart requests on page 3231](#)
- [diagnose sys scanunit auto-restart reset on page 3232](#)
- [diagnose sys scanunit auto-restart status on page 3232](#)
- [diagnose sys scanunit auto-restart time on page 3232](#)
- [diagnose sys scanunit av on page 3232](#)
- [diagnose sys scanunit av filetype-reuse on page 3232](#)
- [diagnose sys scanunit av filetype-reuse disable on page 3233](#)
- [diagnose sys scanunit av filetype-reuse enable on page 3233](#)
- [diagnose sys scanunit av reload-avdb on page 3233](#)
- [diagnose sys scanunit av reload-aveng on page 3233](#)
- [diagnose sys scanunit av reload-fsa-ext on page 3233](#)
- [diagnose sys scanunit bypass on page 3233](#)
- [diagnose sys scanunit bypass clear on page 3234](#)
- [diagnose sys scanunit bypass disable on page 3234](#)
- [diagnose sys scanunit bypass disable category on page 3234](#)
- [diagnose sys scanunit bypass disable category all on page 3234](#)
- [diagnose sys scanunit bypass disable category av-engine on page 3234](#)
- [diagnose sys scanunit bypass disable category scanunit on page 3234](#)
- [diagnose sys scanunit bypass disable protocol on page 3235](#)
- [diagnose sys scanunit bypass disable protocol all on page 3235](#)
- [diagnose sys scanunit bypass disable protocol cifs on page 3235](#)
- [diagnose sys scanunit bypass disable protocol ftp on page 3235](#)
- [diagnose sys scanunit bypass disable protocol http on page 3235](#)
- [diagnose sys scanunit bypass disable protocol imap on page 3235](#)
- [diagnose sys scanunit bypass disable protocol nntp on page 3236](#)
- [diagnose sys scanunit bypass disable protocol pop3 on page 3236](#)
- [diagnose sys scanunit bypass disable protocol smtp on page 3236](#)
- [diagnose sys scanunit bypass enable on page 3236](#)
- [diagnose sys scanunit bypass enable category on page 3236](#)
- [diagnose sys scanunit bypass enable category all on page 3236](#)
- [diagnose sys scanunit bypass enable category av-engine on page 3237](#)
- [diagnose sys scanunit bypass enable category scanunit on page 3237](#)
- [diagnose sys scanunit bypass enable protocol on page 3237](#)
- [diagnose sys scanunit bypass enable protocol all on page 3237](#)
- [diagnose sys scanunit bypass enable protocol cifs on page 3237](#)
- [diagnose sys scanunit bypass enable protocol ftp on page 3237](#)
- [diagnose sys scanunit bypass enable protocol http on page 3238](#)

- [diagnose sys scanunit bypass enable protocol imap on page 3238](#)
- [diagnose sys scanunit bypass enable protocol nntp on page 3238](#)
- [diagnose sys scanunit bypass enable protocol pop3 on page 3238](#)
- [diagnose sys scanunit bypass enable protocol smtp on page 3238](#)
- [diagnose sys scanunit bypass show on page 3238](#)
- [diagnose sys scanunit cfg on page 3239](#)
- [diagnose sys scanunit cfg clear on page 3239](#)
- [diagnose sys scanunit cfg list on page 3239](#)
- [diagnose sys scanunit crash-dump on page 3239](#)
- [diagnose sys scanunit crash-dump clear on page 3239](#)
- [diagnose sys scanunit crash-dump disable on page 3239](#)
- [diagnose sys scanunit crash-dump enable on page 3240](#)
- [diagnose sys scanunit crash-dump read on page 3240](#)
- [diagnose sys scanunit debug on page 3240](#)
- [diagnose sys scanunit debug all on page 3240](#)
- [diagnose sys scanunit debug analytics on page 3240](#)
- [diagnose sys scanunit debug antispam on page 3241](#)
- [diagnose sys scanunit debug daemon on page 3241](#)
- [diagnose sys scanunit debug dlp on page 3241](#)
- [diagnose sys scanunit debug fhl on page 3241](#)
- [diagnose sys scanunit debug file-filter on page 3241](#)
- [diagnose sys scanunit debug icb on page 3242](#)
- [diagnose sys scanunit debug job on page 3242](#)
- [diagnose sys scanunit debug level on page 3242](#)
- [diagnose sys scanunit debug level error on page 3242](#)
- [diagnose sys scanunit debug level info on page 3242](#)
- [diagnose sys scanunit debug level verbose on page 3243](#)
- [diagnose sys scanunit debug level warning on page 3243](#)
- [diagnose sys scanunit debug outbreak-prevention on page 3243](#)
- [diagnose sys scanunit debug quarantine on page 3243](#)
- [diagnose sys scanunit debug reset on page 3243](#)
- [diagnose sys scanunit debug sane on page 3244](#)
- [diagnose sys scanunit debug show on page 3244](#)
- [diagnose sys scanunit debug start on page 3244](#)
- [diagnose sys scanunit debug stop on page 3244](#)
- [diagnose sys scanunit dlp on page 3244](#)
- [diagnose sys scanunit dlp config on page 3244](#)
- [diagnose sys scanunit dlp config build on page 3245](#)
- [diagnose sys scanunit dlp config status on page 3245](#)
- [diagnose sys scanunit dlp config term on page 3245](#)
- [diagnose sys scanunit dlp reset on page 3245](#)
- [diagnose sys scanunit dlp status on page 3245](#)
- [diagnose sys scanunit dlp threshold on page 3245](#)

- [diagnose sys scanunit file-hash on page 3246](#)
- [diagnose sys scanunit file-hash list on page 3246](#)
- [diagnose sys scanunit file-hash list all on page 3246](#)
- [diagnose sys scanunit file-hash list md5 on page 3246](#)
- [diagnose sys scanunit file-hash list sha1 on page 3246](#)
- [diagnose sys scanunit file-hash list sha256 on page 3246](#)
- [diagnose sys scanunit file-hash query on page 3247](#)
- [diagnose sys scanunit file-hash query md5 on page 3247](#)
- [diagnose sys scanunit file-hash query sha1 on page 3247](#)
- [diagnose sys scanunit file-hash query sha256 on page 3247](#)
- [diagnose sys scanunit file-hash status on page 3247](#)
- [diagnose sys scanunit filter on page 3248](#)
- [diagnose sys scanunit filter clear on page 3248](#)
- [diagnose sys scanunit filter list on page 3248](#)
- [diagnose sys scanunit filter negate on page 3248](#)
- [diagnose sys scanunit filter negate vd on page 3248](#)
- [diagnose sys scanunit filter negate worker on page 3248](#)
- [diagnose sys scanunit filter vd on page 3249](#)
- [diagnose sys scanunit filter worker on page 3249](#)
- [diagnose sys scanunit info on page 3249](#)
- [diagnose sys scanunit info shared_status on page 3249](#)
- [diagnose sys scanunit log on page 3249](#)
- [diagnose sys scanunit log filter on page 3250](#)
- [diagnose sys scanunit log filter clear on page 3250](#)
- [diagnose sys scanunit log filter list on page 3250](#)
- [diagnose sys scanunit log filter negate on page 3250](#)
- [diagnose sys scanunit log filter negate vd on page 3250](#)
- [diagnose sys scanunit log filter negate worker on page 3250](#)
- [diagnose sys scanunit log filter vd on page 3251](#)
- [diagnose sys scanunit log filter worker on page 3251](#)
- [diagnose sys scanunit memory on page 3251](#)
- [diagnose sys scanunit memory conserve on page 3251](#)
- [diagnose sys scanunit memory conserve enter on page 3251](#)
- [diagnose sys scanunit memory conserve exit on page 3252](#)
- [diagnose sys scanunit restart on page 3252](#)
- [diagnose sys scanunit simulate-crash on page 3252](#)
- [diagnose sys scanunit simulate-crash lockup-workers on page 3252](#)
- [diagnose sys scanunit simulate-crash lockup-workers all on page 3252](#)
- [diagnose sys scanunit simulate-crash lockup-workers worker on page 3252](#)
- [diagnose sys scanunit simulate-error on page 3253](#)
- [diagnose sys scanunit simulate-error av-engine-delay on page 3253](#)
- [diagnose sys scanunit simulate-error av-error on page 3253](#)
- [diagnose sys scanunit simulate-error av-status on page 3253](#)

- [diagnose sys scanunit simulate-error cdr-error on page 3254](#)
- [diagnose sys scanunit simulate-error reset on page 3254](#)
- [diagnose sys scanunit simulate-error scan-error-code on page 3254](#)
- [diagnose sys scanunit simulate-error status on page 3254](#)
- [diagnose sys scanunit stats on page 3254](#)
- [diagnose sys scanunit stats all on page 3254](#)
- [diagnose sys scanunit stats builder on page 3255](#)
- [diagnose sys scanunit stats clear on page 3255](#)
- [diagnose sys scanunit stats crash on page 3255](#)
- [diagnose sys scanunit stats debug on page 3255](#)
- [diagnose sys scanunit stats list on page 3255](#)
- [diagnose sys scanunit stats manager on page 3255](#)
- [diagnose sys scanunit stats worker on page 3256](#)
- [diagnose sys scanunit valgrind on page 3256](#)
- [diagnose sys scanunit valgrind disable on page 3256](#)
- [diagnose sys scanunit valgrind enable on page 3256](#)
- [diagnose sys scanunit valgrind log on page 3256](#)
- [diagnose sys scanunit valgrind log clear on page 3256](#)
- [diagnose sys scanunit valgrind log show on page 3257](#)
- [diagnose sys scanunit valgrind memcheck on page 3257](#)
- [diagnose sys scanunit valgrind memcheck_less on page 3257](#)
- [diagnose sys scanunit valgrind status on page 3257](#)
- [diagnose sys scanunit vdom-stats on page 3257](#)
- [diagnose sys scanunit vdom-stats all on page 3257](#)
- [diagnose sys scanunit vdom-stats clear on page 3258](#)
- [diagnose sys scanunit vdom-stats clear-all on page 3258](#)
- [diagnose sys scanunit vdom-stats list on page 3258](#)
- [diagnose sys scanunit watchdog-override on page 3258](#)
- [diagnose sys scanunit watchdog-override disable on page 3258](#)
- [diagnose sys scanunit watchdog-override enable on page 3258](#)
- [diagnose sys scanunit watchdog-override interval on page 3259](#)
- [diagnose sys sccp-proxy on page 3259](#)
- [diagnose sys sccp-proxy debug-console on page 3259](#)
- [diagnose sys sccp-proxy phone on page 3259](#)
- [diagnose sys sccp-proxy phone list on page 3259](#)
- [diagnose sys sccp-proxy redirect on page 3259](#)
- [diagnose sys sccp-proxy redirect list on page 3260](#)
- [diagnose sys sccp-proxy restart on page 3260](#)
- [diagnose sys sccp-proxy stats on page 3260](#)
- [diagnose sys sccp-proxy stats clear on page 3260](#)
- [diagnose sys sccp-proxy stats list on page 3260](#)
- [diagnose sys sccp-proxy stats mem on page 3260](#)
- [diagnose sys sccp-proxy stats mem full on page 3261](#)

- [diagnose sys sccp-proxy stats mem summary on page 3261](#)
- [diagnose sys sccp-proxy stats proto on page 3261](#)
- [diagnose sys sccp-proxy valgrind on page 3261](#)
- [diagnose sys sccp-proxy valgrind disable on page 3261](#)
- [diagnose sys sccp-proxy valgrind enable on page 3261](#)
- [diagnose sys sccp-proxy valgrind log on page 3262](#)
- [diagnose sys sccp-proxy valgrind log clear on page 3262](#)
- [diagnose sys sccp-proxy valgrind log show on page 3262](#)
- [diagnose sys sccp-proxy valgrind memcheck on page 3262](#)
- [diagnose sys sccp-proxy valgrind memcheck_less on page 3262](#)
- [diagnose sys sccp-proxy valgrind status on page 3262](#)
- [diagnose sys sdn on page 3263](#)
- [diagnose sys sdn cache on page 3263](#)
- [diagnose sys sdn status on page 3263](#)
- [diagnose sys sdwan on page 3263](#)
- [diagnose sys sdwan advpn on page 3264](#)
- [diagnose sys sdwan advpn-session on page 3264](#)
- [diagnose sys sdwan health-check on page 3264](#)
- [diagnose sys sdwan health-check filter on page 3264](#)
- [diagnose sys sdwan health-check filter clear on page 3264](#)
- [diagnose sys sdwan health-check filter member on page 3264](#)
- [diagnose sys sdwan health-check filter name on page 3265](#)
- [diagnose sys sdwan health-check remote on page 3265](#)
- [diagnose sys sdwan health-check status on page 3265](#)
- [diagnose sys sdwan internet-service-app-ctrl-3t-set on page 3265](#)
- [diagnose sys sdwan internet-service-app-ctrl-3t-unset on page 3266](#)
- [diagnose sys sdwan internet-service-app-ctrl-flush on page 3266](#)
- [diagnose sys sdwan internet-service-app-ctrl-list on page 3266](#)
- [diagnose sys sdwan internet-service-app-ctrl-list app-id on page 3266](#)
- [diagnose sys sdwan internet-service-app-ctrl-list cat-id on page 3267](#)
- [diagnose sys sdwan internet-service-app-ctrl6-3t-set on page 3267](#)
- [diagnose sys sdwan internet-service-app-ctrl6-3t-unset on page 3267](#)
- [diagnose sys sdwan internet-service-app-ctrl6-flush on page 3268](#)
- [diagnose sys sdwan internet-service-app-ctrl6-list on page 3268](#)
- [diagnose sys sdwan internet-service-app-ctrl6-list app-id on page 3268](#)
- [diagnose sys sdwan internet-service-app-ctrl6-list cat-id on page 3268](#)
- [diagnose sys sdwan intf-sla-log on page 3268](#)
- [diagnose sys sdwan log on page 3269](#)
- [diagnose sys sdwan member on page 3269](#)
- [diagnose sys sdwan neighbor on page 3269](#)
- [diagnose sys sdwan reset on page 3269](#)
- [diagnose sys sdwan route on page 3269](#)
- [diagnose sys sdwan route6 on page 3270](#)

- [diagnose sys sdwan service4 on page 3270](#)
- [diagnose sys sdwan service6 on page 3270](#)
- [diagnose sys sdwan sla-log on page 3270](#)
- [diagnose sys sdwan zone on page 3271](#)
- [diagnose sys server-probe on page 3271](#)
- [diagnose sys server-probe response on page 3271](#)
- [diagnose sys service-communication on page 3271](#)
- [diagnose sys session on page 3271](#)
- [diagnose sys session clear on page 3272](#)
- [diagnose sys session exp-stat on page 3272](#)
- [diagnose sys session filter on page 3272](#)
- [diagnose sys session filter clear on page 3272](#)
- [diagnose sys session filter clear dintf on page 3272](#)
- [diagnose sys session filter clear dport on page 3272](#)
- [diagnose sys session filter clear dst on page 3273](#)
- [diagnose sys session filter clear duration on page 3273](#)
- [diagnose sys session filter clear expire on page 3273](#)
- [diagnose sys session filter clear nport on page 3273](#)
- [diagnose sys session filter clear nsrc on page 3273](#)
- [diagnose sys session filter clear policy on page 3273](#)
- [diagnose sys session filter clear proto on page 3274](#)
- [diagnose sys session filter clear proto-state on page 3274](#)
- [diagnose sys session filter clear session-state1 on page 3274](#)
- [diagnose sys session filter clear session-state2 on page 3274](#)
- [diagnose sys session filter clear sintf on page 3274](#)
- [diagnose sys session filter clear sport on page 3274](#)
- [diagnose sys session filter clear src on page 3275](#)
- [diagnose sys session filter clear vd on page 3275](#)
- [diagnose sys session filter dintf on page 3275](#)
- [diagnose sys session filter dport on page 3275](#)
- [diagnose sys session filter dst on page 3275](#)
- [diagnose sys session filter duration on page 3276](#)
- [diagnose sys session filter expire on page 3276](#)
- [diagnose sys session filter ext-dst on page 3276](#)
- [diagnose sys session filter ext-dst-negate on page 3276](#)
- [diagnose sys session filter ext-src on page 3277](#)
- [diagnose sys session filter ext-src-negate on page 3277](#)
- [diagnose sys session filter negate on page 3277](#)
- [diagnose sys session filter negate dintf on page 3277](#)
- [diagnose sys session filter negate dport on page 3277](#)
- [diagnose sys session filter negate dst on page 3278](#)
- [diagnose sys session filter negate duration on page 3278](#)
- [diagnose sys session filter negate expire on page 3278](#)

- [diagnose sys session filter negate nport on page 3278](#)
- [diagnose sys session filter negate nsrc on page 3278](#)
- [diagnose sys session filter negate policy on page 3278](#)
- [diagnose sys session filter negate proto on page 3279](#)
- [diagnose sys session filter negate proto-state on page 3279](#)
- [diagnose sys session filter negate session-state1 on page 3279](#)
- [diagnose sys session filter negate session-state2 on page 3279](#)
- [diagnose sys session filter negate sintf on page 3279](#)
- [diagnose sys session filter negate sport on page 3279](#)
- [diagnose sys session filter negate src on page 3280](#)
- [diagnose sys session filter negate vd on page 3280](#)
- [diagnose sys session filter nport on page 3280](#)
- [diagnose sys session filter nsrc on page 3280](#)
- [diagnose sys session filter policy on page 3280](#)
- [diagnose sys session filter proto on page 3281](#)
- [diagnose sys session filter proto-state on page 3281](#)
- [diagnose sys session filter session-state1 on page 3282](#)
- [diagnose sys session filter session-state2 on page 3282](#)
- [diagnose sys session filter sintf on page 3282](#)
- [diagnose sys session filter sport on page 3282](#)
- [diagnose sys session filter src on page 3283](#)
- [diagnose sys session filter vd on page 3283](#)
- [diagnose sys session filter vd-name on page 3283](#)
- [diagnose sys session full-stat on page 3283](#)
- [diagnose sys session help on page 3283](#)
- [diagnose sys session help add on page 3284](#)
- [diagnose sys session help delete on page 3284](#)
- [diagnose sys session help list on page 3284](#)
- [diagnose sys session list on page 3284](#)
- [diagnose sys session list expectation on page 3284](#)
- [diagnose sys session stat on page 3285](#)
- [diagnose sys session sync on page 3285](#)
- [diagnose sys session sync reset on page 3285](#)
- [diagnose sys session ttl on page 3285](#)
- [diagnose sys session6 on page 3285](#)
- [diagnose sys session6 clear on page 3285](#)
- [diagnose sys session6 exp-stat on page 3286](#)
- [diagnose sys session6 filter on page 3286](#)
- [diagnose sys session6 filter clear on page 3286](#)
- [diagnose sys session6 filter clear dintf on page 3286](#)
- [diagnose sys session6 filter clear dport on page 3286](#)
- [diagnose sys session6 filter clear dst on page 3286](#)
- [diagnose sys session6 filter clear duration on page 3287](#)

- [diagnose sys session6 filter clear expire on page 3287](#)
- [diagnose sys session6 filter clear nport on page 3287](#)
- [diagnose sys session6 filter clear nsrc on page 3287](#)
- [diagnose sys session6 filter clear policy on page 3287](#)
- [diagnose sys session6 filter clear proto on page 3287](#)
- [diagnose sys session6 filter clear proto-state on page 3288](#)
- [diagnose sys session6 filter clear session-state1 on page 3288](#)
- [diagnose sys session6 filter clear session-state2 on page 3288](#)
- [diagnose sys session6 filter clear sintf on page 3288](#)
- [diagnose sys session6 filter clear sport on page 3288](#)
- [diagnose sys session6 filter clear src on page 3288](#)
- [diagnose sys session6 filter clear vd on page 3289](#)
- [diagnose sys session6 filter dintf on page 3289](#)
- [diagnose sys session6 filter dport on page 3289](#)
- [diagnose sys session6 filter dst on page 3289](#)
- [diagnose sys session6 filter duration on page 3289](#)
- [diagnose sys session6 filter expire on page 3290](#)
- [diagnose sys session6 filter ext-dst on page 3290](#)
- [diagnose sys session6 filter ext-dst-negate on page 3290](#)
- [diagnose sys session6 filter ext-src on page 3290](#)
- [diagnose sys session6 filter ext-src-negate on page 3291](#)
- [diagnose sys session6 filter negate on page 3291](#)
- [diagnose sys session6 filter negate dintf on page 3291](#)
- [diagnose sys session6 filter negate dport on page 3291](#)
- [diagnose sys session6 filter negate dst on page 3291](#)
- [diagnose sys session6 filter negate duration on page 3292](#)
- [diagnose sys session6 filter negate expire on page 3292](#)
- [diagnose sys session6 filter negate nport on page 3292](#)
- [diagnose sys session6 filter negate nsrc on page 3292](#)
- [diagnose sys session6 filter negate policy on page 3292](#)
- [diagnose sys session6 filter negate proto on page 3292](#)
- [diagnose sys session6 filter negate proto-state on page 3293](#)
- [diagnose sys session6 filter negate session-state1 on page 3293](#)
- [diagnose sys session6 filter negate session-state2 on page 3293](#)
- [diagnose sys session6 filter negate sintf on page 3293](#)
- [diagnose sys session6 filter negate sport on page 3293](#)
- [diagnose sys session6 filter negate src on page 3293](#)
- [diagnose sys session6 filter negate vd on page 3294](#)
- [diagnose sys session6 filter nport on page 3294](#)
- [diagnose sys session6 filter nsrc on page 3294](#)
- [diagnose sys session6 filter policy on page 3294](#)
- [diagnose sys session6 filter proto on page 3295](#)
- [diagnose sys session6 filter proto-state on page 3295](#)

- [diagnose sys session6 filter session-state1 on page 3295](#)
- [diagnose sys session6 filter session-state2 on page 3295](#)
- [diagnose sys session6 filter sintf on page 3296](#)
- [diagnose sys session6 filter sport on page 3296](#)
- [diagnose sys session6 filter src on page 3296](#)
- [diagnose sys session6 filter vd on page 3296](#)
- [diagnose sys session6 filter vd-name on page 3297](#)
- [diagnose sys session6 full-stat on page 3297](#)
- [diagnose sys session6 help on page 3297](#)
- [diagnose sys session6 help add on page 3297](#)
- [diagnose sys session6 help delete on page 3298](#)
- [diagnose sys session6 help list on page 3298](#)
- [diagnose sys session6 list on page 3298](#)
- [diagnose sys session6 list expectation on page 3298](#)
- [diagnose sys session6 stat on page 3298](#)
- [diagnose sys session6 sync on page 3298](#)
- [diagnose sys session6 sync reset on page 3299](#)
- [diagnose sys shmfile on page 3299](#)
- [diagnose sys shmfile dump on page 3299](#)
- [diagnose sys shmfile dump oid-app on page 3299](#)
- [diagnose sys shmfile dump oid-slab on page 3299](#)
- [diagnose sys shmfile dump slab-file on page 3300](#)
- [diagnose sys shmfile dump table-count on page 3300](#)
- [diagnose sys shmfile dump table-count total on page 3300](#)
- [diagnose sys shmfile dump table-count vdom on page 3300](#)
- [diagnose sys shmfile dump vdom on page 3300](#)
- [diagnose sys sip on page 3301](#)
- [diagnose sys sip debug-mask on page 3301](#)
- [diagnose sys sip dialog on page 3301](#)
- [diagnose sys sip dialog clear on page 3301](#)
- [diagnose sys sip dialog list on page 3301](#)
- [diagnose sys sip mapping on page 3302](#)
- [diagnose sys sip mapping list on page 3302](#)
- [diagnose sys sip status on page 3302](#)
- [diagnose sys sip-proxy on page 3302](#)
- [diagnose sys sip-proxy alg on page 3302](#)
- [diagnose sys sip-proxy alg bypass on page 3302](#)
- [diagnose sys sip-proxy alg parse-only on page 3303](#)
- [diagnose sys sip-proxy calls on page 3303](#)
- [diagnose sys sip-proxy calls clear on page 3303](#)
- [diagnose sys sip-proxy calls idle on page 3303](#)
- [diagnose sys sip-proxy calls invite on page 3303](#)
- [diagnose sys sip-proxy calls list on page 3303](#)

- [diagnose sys sip-proxy config on page 3304](#)
- [diagnose sys sip-proxy config list on page 3304](#)
- [diagnose sys sip-proxy config profiles on page 3304](#)
- [diagnose sys sip-proxy debug-console on page 3304](#)
- [diagnose sys sip-proxy filter on page 3304](#)
- [diagnose sys sip-proxy filter clear on page 3304](#)
- [diagnose sys sip-proxy filter dst-addr4 on page 3305](#)
- [diagnose sys sip-proxy filter dst-addr6 on page 3305](#)
- [diagnose sys sip-proxy filter dst-port on page 3305](#)
- [diagnose sys sip-proxy filter list on page 3305](#)
- [diagnose sys sip-proxy filter negate on page 3306](#)
- [diagnose sys sip-proxy filter negate dst-addr4 on page 3306](#)
- [diagnose sys sip-proxy filter negate dst-addr6 on page 3306](#)
- [diagnose sys sip-proxy filter negate dst-port on page 3306](#)
- [diagnose sys sip-proxy filter negate policy on page 3306](#)
- [diagnose sys sip-proxy filter negate policy-type on page 3306](#)
- [diagnose sys sip-proxy filter negate src-addr4 on page 3307](#)
- [diagnose sys sip-proxy filter negate src-addr6 on page 3307](#)
- [diagnose sys sip-proxy filter negate src-port on page 3307](#)
- [diagnose sys sip-proxy filter negate vd on page 3307](#)
- [diagnose sys sip-proxy filter negate voip-profile on page 3307](#)
- [diagnose sys sip-proxy filter policy on page 3307](#)
- [diagnose sys sip-proxy filter policy-type on page 3308](#)
- [diagnose sys sip-proxy filter policy-type ipv4 on page 3308](#)
- [diagnose sys sip-proxy filter policy-type ipv6 on page 3308](#)
- [diagnose sys sip-proxy filter src-addr4 on page 3308](#)
- [diagnose sys sip-proxy filter src-addr6 on page 3308](#)
- [diagnose sys sip-proxy filter src-port on page 3309](#)
- [diagnose sys sip-proxy filter vd on page 3309](#)
- [diagnose sys sip-proxy filter voip-profile on page 3309](#)
- [diagnose sys sip-proxy log-filter on page 3309](#)
- [diagnose sys sip-proxy log-filter clear on page 3310](#)
- [diagnose sys sip-proxy log-filter dst-addr4 on page 3310](#)
- [diagnose sys sip-proxy log-filter dst-addr6 on page 3310](#)
- [diagnose sys sip-proxy log-filter dst-port on page 3310](#)
- [diagnose sys sip-proxy log-filter list on page 3311](#)
- [diagnose sys sip-proxy log-filter negate on page 3311](#)
- [diagnose sys sip-proxy log-filter negate dst-addr4 on page 3311](#)
- [diagnose sys sip-proxy log-filter negate dst-addr6 on page 3311](#)
- [diagnose sys sip-proxy log-filter negate dst-port on page 3311](#)
- [diagnose sys sip-proxy log-filter negate policy on page 3311](#)
- [diagnose sys sip-proxy log-filter negate policy-type on page 3312](#)
- [diagnose sys sip-proxy log-filter negate src-addr4 on page 3312](#)

- [diagnose sys sip-proxy log-filter negate src-addr6 on page 3312](#)
- [diagnose sys sip-proxy log-filter negate src-port on page 3312](#)
- [diagnose sys sip-proxy log-filter negate vd on page 3312](#)
- [diagnose sys sip-proxy log-filter negate voip-profile on page 3312](#)
- [diagnose sys sip-proxy log-filter policy on page 3313](#)
- [diagnose sys sip-proxy log-filter policy-type on page 3313](#)
- [diagnose sys sip-proxy log-filter policy-type ipv4 on page 3313](#)
- [diagnose sys sip-proxy log-filter policy-type ipv6 on page 3313](#)
- [diagnose sys sip-proxy log-filter src-addr4 on page 3313](#)
- [diagnose sys sip-proxy log-filter src-addr6 on page 3314](#)
- [diagnose sys sip-proxy log-filter src-port on page 3314](#)
- [diagnose sys sip-proxy log-filter vd on page 3314](#)
- [diagnose sys sip-proxy log-filter voip-profile on page 3314](#)
- [diagnose sys sip-proxy meters on page 3315](#)
- [diagnose sys sip-proxy meters list on page 3315](#)
- [diagnose sys sip-proxy redirect on page 3315](#)
- [diagnose sys sip-proxy redirect list on page 3315](#)
- [diagnose sys sip-proxy restart on page 3315](#)
- [diagnose sys sip-proxy scheduler-times on page 3315](#)
- [diagnose sys sip-proxy scheduler-times display on page 3316](#)
- [diagnose sys sip-proxy scheduler-times start on page 3316](#)
- [diagnose sys sip-proxy scheduler-times stop on page 3316](#)
- [diagnose sys sip-proxy session on page 3316](#)
- [diagnose sys sip-proxy session list on page 3316](#)
- [diagnose sys sip-proxy ssl on page 3316](#)
- [diagnose sys sip-proxy ssl hardware on page 3317](#)
- [diagnose sys sip-proxy ssl software on page 3317](#)
- [diagnose sys sip-proxy stats on page 3317](#)
- [diagnose sys sip-proxy stats call on page 3317](#)
- [diagnose sys sip-proxy stats clear on page 3317](#)
- [diagnose sys sip-proxy stats ha on page 3317](#)
- [diagnose sys sip-proxy stats list on page 3318](#)
- [diagnose sys sip-proxy stats mem on page 3318](#)
- [diagnose sys sip-proxy stats mem full on page 3318](#)
- [diagnose sys sip-proxy stats mem summary on page 3318](#)
- [diagnose sys sip-proxy stats proto on page 3318](#)
- [diagnose sys sip-proxy stats ssl-auth on page 3318](#)
- [diagnose sys sip-proxy stats udp on page 3319](#)
- [diagnose sys sip-proxy valgrind on page 3319](#)
- [diagnose sys sip-proxy valgrind disable on page 3319](#)
- [diagnose sys sip-proxy valgrind enable on page 3319](#)
- [diagnose sys sip-proxy valgrind log on page 3319](#)
- [diagnose sys sip-proxy valgrind log clear on page 3319](#)

- [diagnose sys sip-proxy valgrind log show on page 3320](#)
- [diagnose sys sip-proxy valgrind memcheck on page 3320](#)
- [diagnose sys sip-proxy valgrind memcheck_less on page 3320](#)
- [diagnose sys sip-proxy valgrind status on page 3320](#)
- [diagnose sys sip-proxy vdom on page 3320](#)
- [diagnose sys sip-proxy vdom list on page 3320](#)
- [diagnose sys sip-proxy vip on page 3321](#)
- [diagnose sys sip-proxy vip real-server on page 3321](#)
- [diagnose sys speedtest-server on page 3321](#)
- [diagnose sys speedtest-server clients on page 3321](#)
- [diagnose sys speedtest-server clients flush on page 3321](#)
- [diagnose sys speedtest-server clients list on page 3321](#)
- [diagnose sys speedtest-server controller on page 3322](#)
- [diagnose sys speedtest-server controller add on page 3322](#)
- [diagnose sys speedtest-server controller del on page 3322](#)
- [diagnose sys speedtest-server controller list on page 3322](#)
- [diagnose sys speedtest-server log on page 3322](#)
- [diagnose sys speedtest-server log del-file on page 3323](#)
- [diagnose sys speedtest-server log list on page 3323](#)
- [diagnose sys speedtest-server log load-disk on page 3323](#)
- [diagnose sys speedtest-server log save-disk on page 3323](#)
- [diagnose sys speedtest-server speedtest-dbg on page 3323](#)
- [diagnose sys tcp-auth-options on page 3323](#)
- [diagnose sys tcp-option on page 3324](#)
- [diagnose sys tcp-option dump on page 3324](#)
- [diagnose sys tcp-option sack on page 3324](#)
- [diagnose sys tcp-option sack disable on page 3324](#)
- [diagnose sys tcp-option sack enable on page 3324](#)
- [diagnose sys tcp-option timestamps on page 3324](#)
- [diagnose sys tcp-option timestamps disable on page 3325](#)
- [diagnose sys tcp-option timestamps enable on page 3325](#)
- [diagnose sys tcp-option window-scale on page 3325](#)
- [diagnose sys tcp-option window-scale disable on page 3325](#)
- [diagnose sys tcp-option window-scale enable on page 3325](#)
- [diagnose sys tcpsock on page 3325](#)
- [diagnose sys tcpsock6 on page 3326](#)
- [diagnose sys top on page 3326](#)
- [diagnose sys top-all on page 3326](#)
- [diagnose sys top-fd on page 3326](#)
- [diagnose sys top-fd detail on page 3327](#)
- [diagnose sys top-mem on page 3327](#)
- [diagnose sys top-mem detail on page 3327](#)
- [diagnose sys top-sockmem on page 3327](#)

- [diagnose sys traffic on page 3328](#)
- [diagnose sys traffic app-stats on page 3328](#)
- [diagnose sys traffic app-stats add on page 3328](#)
- [diagnose sys traffic app-stats del on page 3328](#)
- [diagnose sys traffic app-stats hash-stats on page 3328](#)
- [diagnose sys traffic app-stats list on page 3329](#)
- [diagnose sys traffic statistics on page 3329](#)
- [diagnose sys traffic statistics clear on page 3329](#)
- [diagnose sys traffic statistics show on page 3329](#)
- [diagnose sys traffic-priority on page 3329](#)
- [diagnose sys traffic-priority list on page 3329](#)
- [diagnose sys udp-reserved-port on page 3330](#)
- [diagnose sys udp-reserved-port test on page 3330](#)
- [diagnose sys udpsock on page 3330](#)
- [diagnose sys udpsock6 on page 3330](#)
- [diagnose sys upgrade-report on page 3330](#)
- [diagnose sys upgrade-report current on page 3330](#)
- [diagnose sys upgrade-report generate on page 3331](#)
- [diagnose sys upgrade-report on-disk on page 3331](#)
- [diagnose sys uuid on page 3331](#)
- [diagnose sys uuid allow-manual-set on page 3331](#)
- [diagnose sys uuid allow-manual-set disable on page 3331](#)
- [diagnose sys uuid allow-manual-set enable on page 3331](#)
- [diagnose sys uuid generate on page 3332](#)
- [diagnose sys var-zone on page 3332](#)
- [diagnose sys var-zone show on page 3332](#)
- [diagnose sys vd on page 3332](#)
- [diagnose sys vd add on page 3332](#)
- [diagnose sys vd delete on page 3332](#)
- [diagnose sys vd list on page 3333](#)
- [diagnose sys vd set on page 3333](#)
- [diagnose sys vd stats on page 3333](#)
- [diagnose sys vdom-property on page 3333](#)
- [diagnose sys vlan on page 3333](#)
- [diagnose sys vlan list on page 3334](#)
- [diagnose sys vxlan on page 3334](#)
- [diagnose sys vxlan device on page 3334](#)
- [diagnose sys vxlan device list on page 3334](#)
- [diagnose sys vxlan fdb on page 3334](#)
- [diagnose sys vxlan fdb list on page 3334](#)
- [diagnose sys vxlan fdb stat on page 3335](#)
- [diagnose sys waninfo on page 3335](#)
- [diagnose sys waninfo ipify on page 3335](#)

- [diagnose sys wccp on page 3335](#)
- [diagnose sys wccp delete on page 3335](#)
- [diagnose sys wccp flush on page 3336](#)
- [diagnose sys wccp list on page 3336](#)

diagnose sys acme

ACME client diagnostics.

```
diagnose sys acme
```

diagnose sys acme add-account

Import an ACME account to 'system acme.accounts'.

```
diagnose sys acme add-account <id> <url> <ca_url> <status> <contact> <privatekey> <passphrase>  
<eab-keyid> <eab-hmac>
```

Parameter	Description	Type	Size
<id>	Account ID.	string	
<url>	Account URL.	string	
<ca_url>	Account CA URL.	string	
<status>	Account Status.	string	
<contact>	Account Email.	string	
<privatekey>	Account PEM private key.	string	
<passphrase>	Account private key passphrase (optional).	string	
<eab-keyid>	Account External Account Binding Key ID (optional).	string	
<eab-hmac>	Account External Account Binding Key HMAC (optional).	string	

diagnose sys acme clear-staging

Force-delete the staging area of the ACME client for a given domain.

```
diagnose sys acme clear-staging <domain>
```

Parameter	Description	Type	Size
<domain>	Certificate's CN domain.	string	

diagnose sys acme debug

Debug output options for the ACME client.

```
diagnose sys acme debug
```

diagnose sys acme debug disable

Disable debug output.

```
diagnose sys acme debug disable
```

diagnose sys acme debug enable

Enable debug output options.

```
diagnose sys acme debug enable
```

diagnose sys acme debug enable level

Set debug level.

```
diagnose sys acme debug enable level
```

diagnose sys acme debug enable level debug

debug

```
diagnose sys acme debug enable level debug
```

diagnose sys acme debug enable level error

error

```
diagnose sys acme debug enable level error
```


diagnose sys acme debug enable level info

info

```
diagnose sys acme debug enable level info
```

diagnose sys acme debug enable level verbose

verbose

```
diagnose sys acme debug enable level verbose
```

diagnose sys acme debug enable level veryverbose

veryverbose

```
diagnose sys acme debug enable level veryverbose
```

diagnose sys acme debug enable level warning

warning

```
diagnose sys acme debug enable level warning
```

diagnose sys acme delete-cert

Delete certificate from the ACME cert store for a given domain.

```
diagnose sys acme delete-cert <domain>
```

Parameter	Description	Type	Size
<domain>	Certificate's CN domain.	string	

diagnose sys acme force-renew

Force the renewal of a certificate.

```
diagnose sys acme force-renew <domain>
```

Parameter	Description	Type	Size
<domain>	Certificate's CN domain. (Empty to clear all force renew flags)	string	

diagnose sys acme list-archive

List the certificate archive.

```
diagnose sys acme list-archive
```

diagnose sys acme list-domains

List certificates currently present in the ACME cert store by CN domain.

```
diagnose sys acme list-domains
```

diagnose sys acme purge-all

Delete the whole ACME cert store, including account data.

```
diagnose sys acme purge-all
```

diagnose sys acme purge-archive

Delete everything in the cert store archive.

```
diagnose sys acme purge-archive
```

diagnose sys acme purge-certs

Delete all certificates from the ACME cert store.

```
diagnose sys acme purge-certs
```

diagnose sys acme regenerate-client-config

Regenerate config for mod_md.

```
diagnose sys acme regenerate-client-config
```

diagnose sys acme regenerate-store

Regenerate store from config.

```
diagnose sys acme regenerate-store
```

diagnose sys acme restart

Gracefully restart Apache.

```
diagnose sys acme restart
```

diagnose sys acme show-archive

Show the certificate archive for a given CN domain.

```
diagnose sys acme show-archive <domain>
```

Parameter	Description	Type	Size
<domain>	Certificate's CN domain.	string	

diagnose sys acme show-client-config

Show config files for mod_md.

```
diagnose sys acme show-client-config
```

diagnose sys acme show-passphrase

Shows the plaintext passphrase of the ACME cert store.

```
diagnose sys acme show-passphrase
```

diagnose sys acme status-full

Fetch the ACME client full status log for a given CN domain.

```
diagnose sys acme status-full <domain>
```

Parameter	Description	Type	Size
<domain>	Certificate's CN domain.	string	

diagnose sys botnet-domain

Botnet domain diagnostics.

```
diagnose sys botnet-domain
```

diagnose sys botnet-domain hit

Botnet domain hits.

```
diagnose sys botnet-domain hit
```

diagnose sys botnet-domain list

List botnet domain entry.

```
diagnose sys botnet-domain list
```

diagnose sys botnet-ip

Botnet IP diagnostics.

```
diagnose sys botnet-ip
```

diagnose sys botnet-ip find

Find botnet IP entry.

```
diagnose sys botnet-ip find <ip> <port> <proto>
```

Parameter	Description	Type	Size
<ip>	IP address.	string	

Parameter	Description	Type	Size
<port>	Port number.	string	
<proto>	Protocol number.	string	

diagnose sys botnet-ip flush

Flush botnet IP entry hit count data.

```
diagnose sys botnet-ip flush
```

diagnose sys botnet-ip hit

Show botnet IP entry hit count data.

```
diagnose sys botnet-ip hit
```

diagnose sys botnet-ip list

List botnet IP entry.

```
diagnose sys botnet-ip list <offset> <number>
```

Parameter	Description	Type	Size
<offset>	Botnet IP entry offset.	string	
<number>	The number of botnet IP entries to display.	string	

diagnose sys certificate-blocklist

Certificate blocklist diagnostics.

```
diagnose sys certificate-blocklist
```

diagnose sys certificate-blocklist count

Get number of entries in malware certificate blocklist.

```
diagnose sys certificate-blocklist count
```

diagnose sys certificate-blocklist delete-mcdb

Delete malicious certificate database.

```
diagnose sys certificate-blocklist delete-mcdb
```

diagnose sys certificate-blocklist query

Query with a certificate hash.

```
diagnose sys certificate-blocklist query <value>
```

Parameter	Description	Type	Size
<value>	SHA1 hash	string	

diagnose sys certificate-blocklist read-range

List entries in malware certificate blocklist based on starting index and count.

```
diagnose sys certificate-blocklist read-range <start> <count>
```

Parameter	Description	Type	Size
<start>	Index of first element	string	
<count>	Number of elements	string	

diagnose sys certificate-blocklist status

Display certificate blocklist status.

```
diagnose sys certificate-blocklist status
```

diagnose sys cmdb

CMDB related information.

```
diagnose sys cmdb
```

diagnose sys cmdb buf-sz

Show cmdb buffer size.

```
diagnose sys cmdb buf-sz
```

diagnose sys cmdb dump

Dump cmdb internal data.

```
diagnose sys cmdb dump
```

diagnose sys cmdb dump vdom

Dump vdom data.

```
diagnose sys cmdb dump vdom <global/vdom-name>
```

Parameter	Description	Type	Size
<global/vdom-name>	Dump global or vdom-name data details.	string	

diagnose sys cmdb flag

CMDB related flags.

```
diagnose sys cmdb flag
```

diagnose sys cmdb flag info

CMDB related flags information.

```
diagnose sys cmdb flag info
```

diagnose sys cmdb flag reset

Reset CMDB related flags.

```
diagnose sys cmdb flag reset
```

diagnose sys cmdb flag reset script-running

Reset CMDB script-running flag.

```
diagnose sys cmdb flag reset script-running
```

diagnose sys cmdb info

CMDB information.

```
diagnose sys cmdb info
```

diagnose sys cmdb obj-verno

Display object version#.

```
diagnose sys cmdb obj-verno <global|vdom-name> <obj-path> <obj-name>
```

Parameter	Description	Type	Size
<global vdom-name>	global or vdom-name.	string	
<obj-path>	object path.	string	
<obj-name>	object name.	string	

diagnose sys cmdb refcnt

Datasource reference count.

```
diagnose sys cmdb refcnt
```

diagnose sys cmdb refcnt reset

Reset reference count to be consistent with real reference.

```
diagnose sys cmdb refcnt reset <path.object.mkey> <tablename>
```

Parameter	Description	Type	Size
<path.object.mkey>	Table.	string	
<tablename>	Entry.	string	

diagnose sys cmdb refcnt show

Show datasource reference details.

```
diagnose sys cmdb refcnt show <path.object.mkey> <tablename>
```

Parameter	Description	Type	Size
<path.object.mkey>	Table.	string	
<tablename>	Entry.	string	

diagnose sys cmdb set-readlock

Set CMDB read lock.

```
diagnose sys cmdb set-readlock
```

diagnose sys cmdb unset-readlock

Unset CMDB read lock.

```
diagnose sys cmdb unset-readlock
```

diagnose sys cmdb-profile

Get CMDB profile information.

```
diagnose sys cmdb-profile
```

diagnose sys cmdb-profile info

Get CMDB profile shm info.

```
diagnose sys cmdb-profile info
```

diagnose sys cmdb-profile node

Get CMDB profile by node.

```
diagnose sys cmdb-profile node <path.object[.attribute]>
```

Parameter	Description	Type	Size
<path.object[.attribute]>	Path to object/attribute.	string	

diagnose sys cmdb-profile reset

Reset CMDB profile shm info.

```
diagnose sys cmdb-profile reset
```

diagnose sys cmdb-profile top10

sort nodes by operator's time

```
diagnose sys cmdb-profile top10
```

diagnose sys cmdb-profile top10 average

sort nodes by operator's average time

```
diagnose sys cmdb-profile top10 average [n]
```

Parameter	Description	Type	Size
[n]	get n nodes' profile (optional, default is 10)	string	

diagnose sys cmdb-profile top10 total

sort nodes by operator's total time

```
diagnose sys cmdb-profile top10 total [n]
```

Parameter	Description	Type	Size
[n]	get n nodes' profile (optional, default is 10)	string	

diagnose sys config-transaction

Config transaction related information.

```
diagnose sys config-transaction
```

diagnose sys config-transaction show

Show config transaction information.

```
diagnose sys config-transaction show
```

diagnose sys config-transaction show entity-by-txn

Show configuration objects being configured by individual transactions.

```
diagnose sys config-transaction show entity-by-txn <txn-id>
```

Parameter	Description	Type	Size
<txn-id>	Transaction ID.	string	

diagnose sys config-transaction show mctx

Show mctx.

```
diagnose sys config-transaction show mctx
```

diagnose sys config-transaction show txn-cli-commands

Show CLI commands used in a given transaction.

```
diagnose sys config-transaction show txn-cli-commands <txn-id>
```

Parameter	Description	Type	Size
<txn-id>	Transaction ID.	string	

diagnose sys config-transaction show txn-entity

Show configuration objects being configured in transactions.

```
diagnose sys config-transaction show txn-entity
```

diagnose sys config-transaction show txn-info

Show config transaction details.

```
diagnose sys config-transaction show txn-info
```

diagnose sys config-transaction show txn-lock

Show transaction lock status.

```
diagnose sys config-transaction show txn-lock
```

diagnose sys config-transaction show txn-meta

Show config transaction meta information.

```
diagnose sys config-transaction show txn-meta
```

diagnose sys config-transaction status

Show config transaction status in current CLI.

```
diagnose sys config-transaction status
```

diagnose sys cpuset

cpuset

```
diagnose sys cpuset
```

diagnose sys cpuset interrupt

cpuset of interrupt

```
diagnose sys cpuset interrupt <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	id of an interrupt	string	
<xxx>	cpuset mask	string	

diagnose sys cpuset process

cpuset of process

```
diagnose sys cpuset process <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	pid of a process	string	
<xxx>	cpuset mask	string	

diagnose sys csf

Security Fabric diagnostics.

```
diagnose sys csf
```

diagnose sys csf authorization

Authorization requests and permits.

```
diagnose sys csf authorization
```

diagnose sys csf authorization accept

Authorize device to join CSF tree.

```
diagnose sys csf authorization accept <SN> [Name]
```

Parameter	Description	Type	Size
<SN>	Serial number.	string	
[Name]	Optional entry name (if not passed SN is used).	string	

diagnose sys csf authorization deny

Deny device from joining CSF tree.

```
diagnose sys csf authorization deny <SN> [Name]
```

Parameter	Description	Type	Size
<SN>	Serial number.	string	
[Name]	Optional entry name (if not passed SN is used).	string	

diagnose sys csf authorization pending-list

List of pending requests to join security fabric.

```
diagnose sys csf authorization pending-list
```

diagnose sys csf downstream

Show connected downstream FortiGates.

```
diagnose sys csf downstream [-x] [-a]
```

Parameter	Description	Type	Size
[-x]	Show encrypted tokens	string	
[-a]	Show all devices	string	

diagnose sys csf downstream-devices

Show downstream fabric device.

```
diagnose sys csf downstream-devices <device type> [vdom] [group]
```

Parameter	Description	Type	Size
<device type>	fabric device type (e.g. fortinac, fortimail, fortivoice, any).	string	
[vdom]	Connecting VDOM.	string	
[group]	CSF key group.	string	

diagnose sys csf dynamic-sync-read

Read incoming dynamic sync data updates

```
diagnose sys csf dynamic-sync-read <count>
```

Parameter	Description	Type	Size
<count>	Number of updates to read	string	

diagnose sys csf dynamic-sync-request

Get the current dynamic sync data from csfd

```
diagnose sys csf dynamic-sync-request
```

diagnose sys csf dynamic-sync-update

Change the dynamic sync update data

```
diagnose sys csf dynamic-sync-update <content> <count>
```

Parameter	Description	Type	Size
<content>	New data content string	string	
<count>	Number of times to repeat the content string line	string	

diagnose sys csf fabric-device

Debug fabric device handling.

```
diagnose sys csf fabric-device
```

diagnose sys csf fabric-device list

List all known fabric devices.

```
diagnose sys csf fabric-device list
```

diagnose sys csf file

csfd file management.

```
diagnose sys csf file
```

diagnose sys csf file cat

Dump file.

```
diagnose sys csf file cat <name>
```

Parameter	Description	Type	Size
<name>	Name of the file to be dumped.	string	

diagnose sys csf file top-mem

Display largest files.

```
diagnose sys csf file top-mem [count]
```

Parameter	Description	Type	Size
[count]	Number of files to be displayed ([1 - 20] default = 5).	string	

diagnose sys csf forticloud-id-list

List of FortiCloud IDs of downstreams.

```
diagnose sys csf forticloud-id-list
```

diagnose sys csf get-bulk-global-view

Request global view file

```
diagnose sys csf get-bulk-global-view [refresh seconds]
```

Parameter	Description	Type	Size
[refresh seconds]	Acceptable age for cached global file in seconds.	string	

diagnose sys csf global

Show a summary of all connected members in Security Fabric.

```
diagnose sys csf global
```


diagnose sys csf initialize-cmd

send an init command for merge.

```
diagnose sys csf initialize-cmd <path> <cmdb_path> <cmdb_table>
```

Parameter	Description	Type	Size
<path>	fabric path made of serial numbers e.g: SNCURRENT:SNMIDDLE:SNDestination.	string	
<cmdb_path>	path for cmdb table	string	
<cmdb_table>	cmdb table name	string	

diagnose sys csf merge-cmd

send a merge command to downstream.

```
diagnose sys csf merge-cmd <path> <cmdb_path> <cmdb_table> <key> <new_key>
```

Parameter	Description	Type	Size
<path>	fabric path made of serial numbers e.g: SNCURRENT:SNMIDDLE:SNDestination.	string	
<cmdb_path>	path for cmdb table	string	
<cmdb_table>	cmdb table name	string	
<key>	current entry name	string	
<new_key>	new entry name	string	

diagnose sys csf neighbor

CSF enabled devices in adjacency.

```
diagnose sys csf neighbor
```

diagnose sys csf neighbor flush

Clear discovered physical addresses of adjacent devices.

```
diagnose sys csf neighbor flush [interface]
```

Parameter	Description	Type	Size
[interface]	Receiving local interface name.	string	

diagnose sys csf neighbor list

List discovered physical addresses of adjacent devices.

```
diagnose sys csf neighbor list [interface]
```

Parameter	Description	Type	Size
[interface]	Receiving local interface name.	string	

diagnose sys csf query

Query through CSF.

```
diagnose sys csf query <path> [-pt]
```

Parameter	Description	Type	Size
<path>	FGT1(SN):FGT2(SN):...:FGTn(SN)	string	
[-pt]	-p:Partial process. -t:Send health check ping request.	string	

diagnose sys csf ratelimit-test-sender

Floods a socket tunnel to test rate limit behaviour.

```
diagnose sys csf ratelimit-test-sender <serial>
```

Parameter	Description	Type	Size
<serial>	Serial number of destination FortiGate.	string	

diagnose sys csf ratelimit-test-server

A dummy server for the unix tunnel rate limit testing to work against.

```
diagnose sys csf ratelimit-test-server <close-delay-seconds>
```

Parameter	Description	Type	Size
<close-delay-seconds>	Seconds to keep the client socket open after accepting it.	string	

diagnose sys csf send-test-log-upstream

Send a test log to upstream

```
diagnose sys csf send-test-log-upstream
```

diagnose sys csf seqpacket-message-listener

Read a line over a tunneled seqpacket socket.

```
diagnose sys csf seqpacket-message-listener <all|root|upstream|downstream>
```

Parameter	Description	Type	Size
<all root upstream downstream>	Client FortiGates to allow.	string	

diagnose sys csf seqpacket-message-sender

Read a line over a tunneled seqpacket socket.

```
diagnose sys csf seqpacket-message-sender <serial> <all|root|upstream|downstream>
```

Parameter	Description	Type	Size
<serial>	Serial number of destination FortiGate.	string	
<all root upstream downstream>	Allow mode of the destination.	string	

diagnose sys csf stream-message-listener

Read a line over a tunneled stream socket

```
diagnose sys csf stream-message-listener <all|root|upstream|downstream>
```

Parameter	Description	Type	Size
<all root upstream downstream>	Client FortiGates to allow.	string	

diagnose sys csf stream-message-sender

Read a line over a tunneled stream socket.

```
diagnose sys csf stream-message-sender <serial> <all|root|upstream|downstream>
```

Parameter	Description	Type	Size
<serial>	Serial number of destination FortiGate.	string	
<all root upstream downstream>	Allow mode of the destination.	string	

diagnose sys csf trigger-info-update

Trigger an info file update

```
diagnose sys csf trigger-info-update <groups>
```

Parameter	Description	Type	Size
<groups>	CSF key groups in hex	string	

diagnose sys csf tunnel-test-listener

Test the reliable tunnel, listener side

```
diagnose sys csf tunnel-test-listener
```

diagnose sys csf tunnel-test-sender

Test the reliable tunnel, sender side

```
diagnose sys csf tunnel-test-sender <target-sn> <msg-content> <repeats>
```

Parameter	Description	Type	Size
<target-sn>	SN to send the message to	string	
<msg-content>	Content of the message	string	
<repeats>	Number of times to repeat the message	string	

diagnose sys csf upstream

Show connected upstream FortiGates.

```
diagnose sys csf upstream
```

diagnose sys csf versions

get latest incremental version of CSF groups.

```
diagnose sys csf versions
```

diagnose sys csum

System checksum.

```
diagnose sys csum <file>
```

Parameter	Description	Type	Size
<file>	File name.	string	

diagnose sys dayst-info

Daylight saving time information.

```
diagnose sys dayst-info <timezone db name> [year]
```

Parameter	Description	Type	Size
<timezone db name>	Timezone Database Name.	string	
[year]	year	string	

diagnose sys device

Virtual domain device management.

```
diagnose sys device
```

diagnose sys device add

Add device to Virtual Domain.

```
diagnose sys device add <vdname> <devname>
```

Parameter	Description	Type	Size
<vdname>	Virtual Domain Name.	string	
<devname>	Device Name.	string	

diagnose sys device delete

Delete device from Virtual Domain.

```
diagnose sys device delete <vdname> <devname>
```

Parameter	Description	Type	Size
<vdname>	Virtual Domain Name.	string	
<devname>	Device Name.	string	

diagnose sys device list

List devices in Virtual Domain.

```
diagnose sys device list <vdname>
```

Parameter	Description	Type	Size
<vdname>	Virtual Domain Name.	string	

diagnose sys dump-conserve-info

Dump all conserve related info to disk.

```
diagnose sys dump-conserve-info
```

diagnose sys emac-vlan

EMAC VLAN diagnostics.

```
diagnose sys emac-vlan
```

diagnose sys emac-vlan fdb

EMAC VLAN forwarding DB.

```
diagnose sys emac-vlan fdb
```

diagnose sys emac-vlan fdb list

Display EMAC VLAN forwarding DB.

```
diagnose sys emac-vlan fdb list <string>
```

Parameter	Description	Type	Size
<string>	Interface name.	string	

diagnose sys emac-vlan stat

Statistics of EMAC VLAN interfaces.

```
diagnose sys emac-vlan stat <string>
```

Parameter	Description	Type	Size
<string>	Underlying interface name.	string	

diagnose sys external-address-resource

External address resource.

```
diagnose sys external-address-resource
```

diagnose sys external-address-resource list

list

```
diagnose sys external-address-resource list <name>
```

Parameter	Description	Type	Size
<name>	External address resource name.	string	

diagnose sys external-generic-address-resource

External generic address resource.

```
diagnose sys external-generic-address-resource
```

diagnose sys external-generic-address-resource remove-by-name

Remove specific external generic address entry.

```
diagnose sys external-generic-address-resource remove-by-name <name>
```

Parameter	Description	Type	Size
<name>	External generic address entry name.	string	

diagnose sys external-generic-address-resource remove-by-namespace

Remove external generic addresses by namespace.

```
diagnose sys external-generic-address-resource remove-by-namespace <name>
```

Parameter	Description	Type	Size
<name>	External generic address namespace.	string	

diagnose sys external-mac-resource

External mac resource.

```
diagnose sys external-mac-resource
```


diagnose sys external-mac-resource list

list

```
diagnose sys external-mac-resource list <name>
```

Parameter	Description	Type	Size
<name>	External mac resource name.	string	

diagnose sys external-resource

External resource.

```
diagnose sys external-resource
```

diagnose sys external-resource list

Dump external resource file by name.

```
diagnose sys external-resource list <name>
```

Parameter	Description	Type	Size
<name>	Name of external resource.	string	

diagnose sys external-resource push-add

Add entry to external resource set to push updates.

```
diagnose sys external-resource push-add
```

diagnose sys external-resource push-api-json-commands

Test push commands JSON API

```
diagnose sys external-resource push-api-json-commands <COMMANDS-JSON>
```

Parameter	Description	Type	Size
<COMMANDS-JSON>	JSON string for commands.	string	

diagnose sys external-resource push-remove

Remove entry to push external resource set to push updates.

```
diagnose sys external-resource push-remove
```

diagnose sys external-resource push-snapshot

Overwrite external resource set to push updates.

```
diagnose sys external-resource push-snapshot
```

diagnose sys external-resource stats

Display external resource file info.

```
diagnose sys external-resource stats <name>
```

Parameter	Description	Type	Size
<name>	Name of external resource.	string	

diagnose sys filesystem

File system.

```
diagnose sys filesystem
```

diagnose sys filesystem hash

Generate hash for files within the filesystem.

```
diagnose sys filesystem hash
```

diagnose sys filesystem last-modified-files

List the last modified files.

```
diagnose sys filesystem last-modified-files [path] [number]
```

Parameter	Description	Type	Size
[path]	Path for listing modified files (default = /data).	string	
[number]	Number of files to list (default = 10).	string	

diagnose sys filesystem lsof

List open files

```
diagnose sys filesystem lsof
```

diagnose sys filesystem open-files

List open files.

```
diagnose sys filesystem open-files [path]
```

Parameter	Description	Type	Size
[path]	Path of file or directory to check against.	string	

diagnose sys filesystem tree

List the top files/folders tree.

```
diagnose sys filesystem tree [path] [number]
```

Parameter	Description	Type	Size
[path]	Path for listing files/folder (default = /var/log).	string	
[number]	Number of files in each current folder and subfolder to be listed (default = 10).	string	

diagnose sys fips

FIPS mode.

```
diagnose sys fips
```

diagnose sys fips error-mode

Go to error mode.

```
diagnose sys fips error-mode
```

diagnose sys fips kat-error

Force test failure at next self-test.

```
diagnose sys fips kat-error <KAT>
```

Parameter	Description	Type	Size
<KAT>	KAT, empty to display available values.	string	

diagnose sys flash

Flash image.

```
diagnose sys flash
```

diagnose sys flash format

format shared data partition (flash partition #2)

```
diagnose sys flash format
```

diagnose sys flash list

List flash images.

```
diagnose sys flash list <file>
```

Parameter	Description	Type	Size
<file>	List files.	string	

diagnose sys forticonverter

FortiConverter config conversion service diagnostics.

```
diagnose sys forticonverter set-prompt-visibility
```

Parameter	Description	Type	Size
set-prompt-visibility	Set the visibility for the FortiConverter wizard on login.	option	

diagnose sys forticonverter available-source-devices

Retrieve known source device options for a ticket.

```
diagnose sys forticonverter available-source-devices <ticket-id>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to retrieve device information for.	string	

diagnose sys forticonverter create-ticket

Create a ticket for FortiConverter conversion services.

```
diagnose sys forticonverter create-ticket
```

diagnose sys forticonverter custom-create-ticket

Use the custom request API to create a ticket for FortiConverter conversion services.

```
diagnose sys forticonverter custom-create-ticket
```

diagnose sys forticonverter download-status

Get current download status.

```
diagnose sys forticonverter download-status <ticket-id> <extension>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to check for download status	string	
<extension>	Extension of the file to check.	string	

diagnose sys forticonverter eligibility-status

Show current FortiConverter eligibility status.

```
diagnose sys forticonverter eligibility-status
```

diagnose sys forticonverter get-prompt-visibility

Read the visibility status for the FortiConverter wizard on login.

```
diagnose sys forticonverter get-prompt-visibility
```

diagnose sys forticonverter result-availability

Retrieve result file availability status for a ticket.

```
diagnose sys forticonverter result-availability <ticket-id> <extension>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to retrieve result availability for.	string	
<extension>	File extension to retrieve availability for.	string	

diagnose sys forticonverter set-source-fortigate

Set the source FortiGate for a FortiConverter ticket.

```
diagnose sys forticonverter set-source-fortigate <ticket-id> <source-serial>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to set the source FortiGate for.	string	
<source-serial>	Serial number of the source FortiGate.	string	

diagnose sys forticonverter source-config-upload-status

Retrieve source config upload status for a draft ticket.

```
diagnose sys forticonverter source-config-upload-status <ticket-id>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to retrieve source config upload status info for.	string	

diagnose sys forticonverter source-interfaces

Retrieve source interface JSON for a draft ticket.

```
diagnose sys forticonverter source-interfaces <ticket-id>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to retrieve interface information for.	string	

diagnose sys forticonverter start-download

Start download of config from a ticket.

```
diagnose sys forticonverter start-download <ticket-id> <extension>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to download from.	string	
<extension>	Extension of the file to download.	string	

diagnose sys forticonverter submitted-info

Retrieve previously submitted info for a draft ticket.

```
diagnose sys forticonverter submitted-info <ticket-id>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to retrieve submitted info for.	string	

diagnose sys forticonverter update-eligibility

Request updated eligibility status from FortiConverter.

```
diagnose sys forticonverter update-eligibility
```

diagnose sys forticonverter update-result-availability

Request updated result availability from FortiConverter.

```
diagnose sys forticonverter update-result-availability
```

diagnose sys forticonverter upload-local-config

Upload local config to a ticket for this FGT. Debugging purposes only.

```
diagnose sys forticonverter upload-local-config <ticket-id>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to upload config to.	string	

diagnose sys forticonverter upload-status

Retrieve upload status for a ticket.

```
diagnose sys forticonverter upload-status <ticket-id>
```

Parameter	Description	Type	Size
<ticket-id>	Ticket ID to upload config to.	string	

diagnose sys frag-mem

Display memory usage of fragment processing.

```
diagnose sys frag-mem
```


diagnose sys fullcone

Fullcone diagnostics.

```
diagnose sys fullcone
```

diagnose sys geneve

GENEVE diagnostics.

```
diagnose sys geneve
```

diagnose sys geneve list

Display GENEVE devices.

```
diagnose sys geneve list
```

diagnose sys geneve stat

Display GENEVE statistics.

```
diagnose sys geneve stat
```

diagnose sys gre

GRE diagnostics.

```
diagnose sys gre
```

diagnose sys gre keepalive

Keepalive status in GRE tunnels.

```
diagnose sys gre keepalive <name | all>
```

Parameter	Description	Type	Size
<name all>	GRE tunnel name	string	

diagnose sys gre list

List GRE tunnels.

```
diagnose sys gre list
```

diagnose sys h323

H323 diagnostics.

```
diagnose sys h323
```

diagnose sys h323 call

H323 calls.

```
diagnose sys h323 call
```

diagnose sys h323 call list

List H323 calls.

```
diagnose sys h323 call list
```

diagnose sys h323 debug-mask

Mask for H323 kernel trace.

```
diagnose sys h323 debug-mask <mask>
```

Parameter	Description	Type	Size
<mask>	0-disable, 1-parser, 2-CS, 4-RAS, 8-h245.	string	

diagnose sys h323 peer

H323 peers.

```
diagnose sys h323 peer
```

diagnose sys h323 peer list

List H323 peers.

```
diagnose sys h323 peer list
```

diagnose sys h323 status

Display h323 status.

```
diagnose sys h323 status
```

diagnose sys ha

High availability.

```
diagnose sys ha
```

diagnose sys ha autoscale-peers

Show autoscale peers.

```
diagnose sys ha autoscale-peers <Enter> or <vdom-name>
```

Parameter	Description	Type	Size
<Enter> or <vdom-name>	<Enter> to show peers' information in management VDOM, <vdom-name> to show peers' information in specific VDOM.	string	

diagnose sys ha check-vc

check-vc

```
diagnose sys ha check-vc
```

diagnose sys ha checksum

checksum.

```
diagnose sys ha checksum
```

diagnose sys ha checksum autoscale-cluster

Show autoscale cluster checksum.

```
diagnose sys ha checksum autoscale-cluster
```

diagnose sys ha checksum cached

Show HA cached checksum.

```
diagnose sys ha checksum cached <global/vdom-name>
```

Parameter	Description	Type	Size
<global/vdom-name>	Show global or a specific vdom's cached HA checksum.	string	

diagnose sys ha checksum cluster

Show HA cluster checksum by serial number.

```
diagnose sys ha checksum cluster
```

diagnose sys ha checksum log

Enable/disable log.

```
diagnose sys ha checksum log
```

diagnose sys ha checksum log clear

Clear log.

```
diagnose sys ha checksum log clear
```

diagnose sys ha checksum log disable

Disable log.

```
diagnose sys ha checksum log disable
```

diagnose sys ha checksum log enable

Enable log.

```
diagnose sys ha checksum log enable
```

diagnose sys ha checksum recalculate

Re-calculate HA checksum.

```
diagnose sys ha checksum recalculate <Enter> or <global/vdom-name>
```

Parameter	Description	Type	Size
<Enter> or <global/vdom-name>	<Enter> to re-calculate all checksums, or global/vdom-name to re-calculate global or a specific vdom HA checksum.	string	

diagnose sys ha checksum show

Show HA checksum.

```
diagnose sys ha checksum show <Enter> or <global/vdom-name> <Enter> or <object-fullpath> <Enter> or <entry-name>
```

Parameter	Description	Type	Size
<Enter> or <global/vdom-name>	<Enter> to show system checksum; <global/vdom-name> to show global/vdom-name detail checksum.	string	
<Enter> or <object-fullpath>	<Enter> to show objects checksum; <object-fullpath> to show individual object's detail checksum.	string	
<Enter> or <entry-name>	<Enter> to show the specific object's detail checksum; <entry-name> to show a single entry's detail checksum.	string	

diagnose sys ha checksum show-nonsync

Show non-sync HA checksum.

```
diagnose sys ha checksum show-nonsync
```

diagnose sys ha checksum test

test.

```
diagnose sys ha checksum test
```

diagnose sys ha dump-by

Dump HA data by name.

```
diagnose sys ha dump-by
```

diagnose sys ha dump-by debug-zone

Dump HA debug zone.

```
diagnose sys ha dump-by debug-zone
```

diagnose sys ha dump-by device

Dump HA device.

```
diagnose sys ha dump-by device
```

diagnose sys ha dump-by group

Dump all group.

```
diagnose sys ha dump-by group
```

diagnose sys ha dump-by kernel

Dump HA kernel info.

```
diagnose sys ha dump-by kernel
```

diagnose sys ha dump-by rcache

Dump rcache.

```
diagnose sys ha dump-by rcache
```

diagnose sys ha dump-by vcluster

Dump all vcluster.

```
diagnose sys ha dump-by vcluster
```

diagnose sys ha dump-by vdom

Dump HA vdom info.

```
diagnose sys ha dump-by vdom
```

diagnose sys ha extfile-sig

Dump extfile's signature.

```
diagnose sys ha extfile-sig
```

diagnose sys ha fgsp-zone

FGSP zone information.

```
diagnose sys ha fgsp-zone
```

diagnose sys ha fib

FIB information.

```
diagnose sys ha fib
```

diagnose sys ha hactx-stats

HA context statistics

```
diagnose sys ha hactx-stats
```

diagnose sys ha hactx-stats clear

HA context statistics

```
diagnose sys ha hactx-stats clear
```

diagnose sys ha hadiff

HA diff debug.

```
diagnose sys ha hadiff
```

diagnose sys ha hadiff log

Enable/disable log.

```
diagnose sys ha hadiff log
```

diagnose sys ha hadiff log clear

Clear log.

```
diagnose sys ha hadiff log clear
```


diagnose sys ha hadiff log disable

Disable log.

```
diagnose sys ha hadiff log disable
```

diagnose sys ha hadiff log enable

Enable log.

```
diagnose sys ha hadiff log enable
```

diagnose sys ha hadiff max-sync-turns

Set/get max number of sync turns.

```
diagnose sys ha hadiff max-sync-turns <integer>
```

Parameter	Description	Type	Size
<integer>	Set/get max number of sync turns.	string	

diagnose sys ha hadiff max-unsync-wait

Set/get max unsync wait times.

```
diagnose sys ha hadiff max-unsync-wait <integer>
```

Parameter	Description	Type	Size
<integer>	Maximum unsync wait times.	string	

diagnose sys ha hadiff status

HA diff status.

```
diagnose sys ha hadiff status
```

diagnose sys ha hadiff sync-from-higher

enable/disable sync config from higher build.

```
diagnose sys ha hadiff sync-from-higher <Integer>
```

Parameter	Description	Type	Size
<Integer>	the value: 0(=disable), 1(=enable).	string	

diagnose sys ha hasync-conn-max-buf

Set the hasync connection maximum buffer number.

```
diagnose sys ha hasync-conn-max-buf <hasync-conn-max-buf>
```

Parameter	Description	Type	Size
<hasync-conn-max-buf>	Max number of buffers.	string	

diagnose sys ha hasync-stats

hasync daemon stats.

```
diagnose sys ha hasync-stats
```

diagnose sys ha hasync-stats all

Display hasync all objects' stats.

```
diagnose sys ha hasync-stats all
```

diagnose sys ha hasync-stats by-object

Display hasync stats by object.

```
diagnose sys ha hasync-stats by-object <integer>
```

Parameter	Description	Type	Size
<integer>	Object number.	string	

diagnose sys ha hasync-stats most-recent

Display hasync objects recent stats.

```
diagnose sys ha hasync-stats most-recent [integer]
```

Parameter	Description	Type	Size
[integer]	Most recent # of objects to display.	string	

diagnose sys ha hasync-stats most-time

Display hasync objects ranked by total time.

```
diagnose sys ha hasync-stats most-time [integer]
```

Parameter	Description	Type	Size
[integer]	# of top objects to display.	string	

diagnose sys ha heartbeat

Show kernel heartbeat stats.

```
diagnose sys ha heartbeat
```

diagnose sys ha history

Cluster history information.

```
diagnose sys ha history
```

diagnose sys ha history clear

Clear cluster history.

```
diagnose sys ha history clear
```

diagnose sys ha history read

Display cluster history.

```
diagnose sys ha history read
```

diagnose sys ha mac

Mac Information.

```
diagnose sys ha mac
```

diagnose sys ha pingsvr-secondary-force-reset

Reset HA up time.

```
diagnose sys ha pingsvr-secondary-force-reset
```

diagnose sys ha recalculate-extfile-signature

Recalculate external files signature in hasync daemon.

```
diagnose sys ha recalculate-extfile-signature
```

diagnose sys ha reset-health-status

Reset HA health status.

```
diagnose sys ha reset-health-status
```

diagnose sys ha reset-uptime

Reset HA up time.

```
diagnose sys ha reset-uptime
```

diagnose sys ha reset-uptime-primary-only

Reset HA up time (can take effect on primary unit only).

```
diagnose sys ha reset-uptime-primary-only
```

diagnose sys ha session-sync-dev

Session sync ports.

```
diagnose sys ha session-sync-dev
```

diagnose sys ha session-sync-dev clear

Clear session sync ports.

```
diagnose sys ha session-sync-dev clear
```

diagnose sys ha session-sync-dev set

Configure session sync ports.

```
diagnose sys ha session-sync-dev set
```

diagnose sys ha standalone-peers

Standalone peers on kernel.

```
diagnose sys ha standalone-peers
```

diagnose sys ha standalone-peers reset-stats

Reset standalone peers session/packet type counters in kernel.

```
diagnose sys ha standalone-peers reset-stats
```

diagnose sys ha stats

statistics

```
diagnose sys ha stats
```

diagnose sys ha status

status

```
diagnose sys ha status
```

diagnose sys ha sync-stats

Dump HA sync statistics.

```
diagnose sys ha sync-stats
```

diagnose sys ha sync-stats-reset

Reset HA sync statistics.

```
diagnose sys ha sync-stats-reset
```

diagnose sys ha vlan-hb-monitor

Dump vlan heartbeat monitor list.

```
diagnose sys ha vlan-hb-monitor
```

diagnose sys icap-remote-server

Display remote icap servers status.

```
diagnose sys icap-remote-server
```

diagnose sys icap-remote-server status

List remote icap servers status.

```
diagnose sys icap-remote-server status
```

diagnose sys icb

ICB diagnostics.

```
diagnose sys icb
```

diagnose sys icb debug

Debug settings.

```
diagnose sys icb debug
```

diagnose sys icb debug disable

Disable (reset) level setting.

```
diagnose sys icb debug disable
```

diagnose sys icb debug info

Enable info level setting.

```
diagnose sys icb debug info
```

diagnose sys icb debug show

Show current debug settings.

```
diagnose sys icb debug show
```

diagnose sys icb debug verbose

Enable verbose level setting.

```
diagnose sys icb debug verbose
```

diagnose sys icb stats

Statistics.

```
diagnose sys icb stats
```

diagnose sys icb stats list

List statistics.

```
diagnose sys icb stats list
```

diagnose sys icb status

ICB service status.

```
diagnose sys icb status
```

diagnose sys icb status current

Show ICB service status and current supported file-type list.

```
diagnose sys icb status current
```

diagnose sys iotop

Show disk-accessing processes.

```
diagnose sys iotop <interval>
```

Parameter	Description	Type	Size
<interval>	Print interval in seconds (default to 5). Accept value from 5 to 3600.	string	

diagnose sys ipam

IP Address Management diagnostics.

```
diagnose sys ipam
```

diagnose sys ipam delete

delete

```
diagnose sys ipam delete
```

diagnose sys ipam delete device

Delete device from IPAM server.

```
diagnose sys ipam delete device <sn>
```

Parameter	Description	Type	Size
<sn>	SN of device to delete from IPAM server.	string	

diagnose sys ipam largest-available-subnet

Get the largest currently available subnet size.

```
diagnose sys ipam largest-available-subnet
```

diagnose sys ipam list

list

```
diagnose sys ipam list
```

diagnose sys ipam list entries

List IPAM entries.

```
diagnose sys ipam list entries
```

diagnose sys ipam list free-subnets

List free IPAM subnets.

```
diagnose sys ipam list free-subnets
```

diagnose sys ipsec-aggregate

IPsec aggregate diagnostics.

```
diagnose sys ipsec-aggregate
```

diagnose sys ipsec-aggregate list

List IPsec aggregates.

```
diagnose sys ipsec-aggregate list <name>
```

Parameter	Description	Type	Size
<name>	IPsec aggregate name	string	

diagnose sys kill

Kill the process ID.

```
diagnose sys kill <signal> <pid>
```

Parameter	Description	Type	Size
<signal>	Signal number.	string	
<pid>	Process ID.	string	

diagnose sys link-monitor

Link Monitor.

```
diagnose sys link-monitor
```

diagnose sys link-monitor filter

Filter link-monitor

```
diagnose sys link-monitor filter
```

diagnose sys link-monitor filter clear

Clear all filters.

```
diagnose sys link-monitor filter clear
```

diagnose sys link-monitor filter name

Link monitor names <name>.

```
diagnose sys link-monitor filter name <name>
```

Parameter	Description	Type	Size
<name>	Link monitor name.	string	

diagnose sys link-monitor interface

interface quality.

```
diagnose sys link-monitor interface <name> <childname>
```

Parameter	Description	Type	Size
<name>	Show details of an interface entry.	string	
<childname>	Child interface name.	string	

diagnose sys link-monitor launch

Launching a link monitor entry manually.

```
diagnose sys link-monitor launch <entry name>
```

Parameter	Description	Type	Size
<entry name>	Entry.	string	

diagnose sys link-monitor reset-monitor

Reset link monitor statistics.

```
diagnose sys link-monitor reset-monitor <name>
```

Parameter	Description	Type	Size
<name>	Link monitor name.	string	

diagnose sys link-monitor sdwan-hc

SD-WAN health-check monitors.

```
diagnose sys link-monitor sdwan-hc <name> <seq>
```

Parameter	Description	Type	Size
<name>	Health check name.	string	
<seq>	Sequence number.	string	

diagnose sys link-monitor sdwan-service

SD-WAN rule monitors.

```
diagnose sys link-monitor sdwan-service <name> <seq>
```

Parameter	Description	Type	Size
<name>	Health check name.	string	
<seq>	Sequence number.	string	

diagnose sys link-monitor shm-band-stats

Read link bandwidth statistics in SHM.

```
diagnose sys link-monitor shm-band-stats <name>
```

Parameter	Description	Type	Size
<name>	Interface name.	string	

diagnose sys link-monitor shm-stats

Read link monitor statistics in SHM.

```
diagnose sys link-monitor shm-stats <name>
```

Parameter	Description	Type	Size
<name>	Link monitor name.	string	

diagnose sys link-monitor status

status

```
diagnose sys link-monitor status <name | all>
```

Parameter	Description	Type	Size
<name all>	Show details of monitor entry.	string	

diagnose sys link-monitor tunnel

tunnel

```
diagnose sys link-monitor tunnel <name | all> <child name>
```

Parameter	Description	Type	Size
<name all>	Show details of tunnel monitor entry.	string	
<child name>	Show details of child monitor for tunnel.	string	

diagnose sys link-monitor zone-intf

quality of interfaces in an SDWAN zone.

```
diagnose sys link-monitor zone-intf <zone name>
```

Parameter	Description	Type	Size
<zone name>	SD-WAN zone name.	string	

diagnose sys link-monitor-passive

Link Monitor passive.

```
diagnose sys link-monitor-passive
```

diagnose sys link-monitor-passive admin

Passive reports measured by the kernel.

```
diagnose sys link-monitor-passive admin
```

diagnose sys link-monitor-passive admin dbg-rpt

Mock kernel report.

```
diagnose sys link-monitor-passive admin dbg-rpt
```

diagnose sys link-monitor-passive admin dbg-rpt reset

reset

```
diagnose sys link-monitor-passive admin dbg-rpt reset <vf> <serial> <app_id> <intf> <origin>  
<reply>
```

Parameter	Description	Type	Size
<vf>	vfid	string	
<serial>	Session serial	string	
<app_id>	Application ID	string	
<intf>	Interface index	string	
<origin>	origin	string	
<reply>	reply	string	

diagnose sys link-monitor-passive admin dbg-rpt retrans

retrans

```
diagnose sys link-monitor-passive admin dbg-rpt retrans <vf> <serial> <app_id> <intf> <origin_cnt>
<origin_total> <reply_cnt> <reply_total>
```

Parameter	Description	Type	Size
<vf>	vfid	string	
<serial>	Session serial	string	
<app_id>	Application ID	string	
<intf>	Interface index	string	
<origin_cnt>	origin_cnt	string	
<origin_total>	origin_total	string	
<reply_cnt>	reply_cnt	string	
<reply_total>	reply_total	string	

diagnose sys link-monitor-passive admin dbg-rpt rtt

rtt

```
diagnose sys link-monitor-passive admin dbg-rpt rtt <vf> <serial> <app_id> <intf> <srt> <nrt>
```

Parameter	Description	Type	Size
<vf>	vfid	string	
<serial>	Session serial	string	
<app_id>	Application ID	string	
<intf>	Interface index	string	
<srt>	Server response time	string	
<nrt>	Network response time	string	

diagnose sys link-monitor-passive admin dbg-rpt syn-retrans

syn-retrans

```
diagnose sys link-monitor-passive admin dbg-rpt syn-retrans <vf> <serial> <app_id> <intf> <origin>
<reply>
```

Parameter	Description	Type	Size
<vf>	vfid	string	
<serial>	Session serial	string	
<app_id>	Application ID	string	
<intf>	Interface index	string	
<origin>	origin	string	
<reply>	reply	string	

diagnose sys link-monitor-passive admin delete

Delete a report.

```
diagnose sys link-monitor-passive admin delete <interface> <application>
```

Parameter	Description	Type	Size
<interface>	Interface device index.	string	
<application>	Internet service or application ID.	string	

diagnose sys link-monitor-passive admin flush

Flush all the reports.

```
diagnose sys link-monitor-passive admin flush
```

diagnose sys link-monitor-passive admin list

List one or all the collected passive reports.

```
diagnose sys link-monitor-passive admin list <interface> <application> <application>
```

Parameter	Description	Type	Size
<interface> <application>	List the passive report by the given interface and application.	string	
<application>	Set the application.	string	

diagnose sys link-monitor-passive admin list by-application

List passive reports and sort by application.

```
diagnose sys link-monitor-passive admin list by-application <application>
```

Parameter	Description	Type	Size
<application>	List reports of the given application.	string	

diagnose sys link-monitor-passive admin list by-interface

List passive reports and sort by interface.

```
diagnose sys link-monitor-passive admin list by-interface <interface>
```

Parameter	Description	Type	Size
<interface>	List reports of the given interface	string	

diagnose sys link-monitor-passive agent

Passive reports measured by agents.

```
diagnose sys link-monitor-passive agent
```

diagnose sys link-monitor-passive agent agent-oif-map

List agent and interface maps.

```
diagnose sys link-monitor-passive agent agent-oif-map
```

diagnose sys link-monitor-passive agent flush

Flush all the collected reports.

```
diagnose sys link-monitor-passive agent flush
```

diagnose sys link-monitor-passive agent flush-app

Flush details of all the applications.

```
diagnose sys link-monitor-passive agent flush-app
```

diagnose sys link-monitor-passive agent list

List all the collected reports.

```
diagnose sys link-monitor-passive agent list
```

diagnose sys link-monitor-passive agent list-app

List details of each application.

```
diagnose sys link-monitor-passive agent list-app
```

diagnose sys link-monitor-passive agent send-report

Mock an agent to send application performance.

```
diagnose sys link-monitor-passive agent send-report <src> <app_id> <app_name> <latency> <jitter>  
<pktloss> <ntt> <srt> <app_err>
```

Parameter	Description	Type	Size
<src>	Agent address.	string	
<app_id>	Application ID.	string	
<app_name>	Application name.	string	
<latency>	Collected latency.	string	
<jitter>	Collected jitter.	string	
<pktloss>	Collected pktloss	string	
<ntt>	Collected ntt.	string	
<srt>	Collected srt.	string	
<app_err>	Collected application errors	string	

diagnose sys link-monitor-passive remote

Passive reports measured by remote peer.

```
diagnose sys link-monitor-passive remote
```

diagnose sys link-monitor-passive remote list

List one or all the collected reports.

```
diagnose sys link-monitor-passive remote list
```

diagnose sys logdisk

Display log disk status.

```
diagnose sys logdisk
```

diagnose sys logdisk purge-log-data

Purge disk log data, including disk logs and FortiView data.

```
diagnose sys logdisk purge-log-data
```

diagnose sys logdisk quota

Show log disk quota info.

```
diagnose sys logdisk quota
```

diagnose sys logdisk smart

Show log disk S.M.A.R.T. info.

```
diagnose sys logdisk smart
```

diagnose sys logdisk status

Display log disk status.

```
diagnose sys logdisk status
```

diagnose sys logdisk status monitor

Monitor log disk status.

```
diagnose sys logdisk status monitor
```

diagnose sys logdisk usage

Show log disk stats.

```
diagnose sys logdisk usage
```

diagnose sys mcast-session

multicast session

```
diagnose sys mcast-session
```

diagnose sys mcast-session clear

Clear the sessions defined by filter.

```
diagnose sys mcast-session clear
```

diagnose sys mcast-session filter

List session with filters.

```
diagnose sys mcast-session filter
```

diagnose sys mcast-session filter clear

Clear session filter.

```
diagnose sys mcast-session filter clear
```

diagnose sys mcast-session filter clear dport

Clear destination port filter.

```
diagnose sys mcast-session filter clear dport
```

diagnose sys mcast-session filter clear dst

Clear destination IP filter.

```
diagnose sys mcast-session filter clear dst
```

diagnose sys mcast-session filter clear proto

Clear protocol filter.

```
diagnose sys mcast-session filter clear proto
```

diagnose sys mcast-session filter clear intf

Clear source interface filter.

```
diagnose sys mcast-session filter clear intf
```

diagnose sys mcast-session filter clear sport

Clear source port filter.

```
diagnose sys mcast-session filter clear sport
```

diagnose sys mcast-session filter clear src

Clear source IP filter.

```
diagnose sys mcast-session filter clear src
```

diagnose sys mcast-session filter clear vd

Clear virtual domain filter.

```
diagnose sys mcast-session filter clear vd
```

diagnose sys mcast-session filter dport

Destination port.

```
diagnose sys mcast-session filter dport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys mcast-session filter dst

Destination IP address.

```
diagnose sys mcast-session filter dst <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP (from).	string	
<xxx.xxx.xxx.xxx>	Destination IP (to).	string	

diagnose sys mcast-session filter negate

Inverse filter.

```
diagnose sys mcast-session filter negate
```

diagnose sys mcast-session filter negate dport

Inverse destination port.

```
diagnose sys mcast-session filter negate dport
```

diagnose sys mcast-session filter negate dst

Inverse destination IP.

```
diagnose sys mcast-session filter negate dst
```

diagnose sys mcast-session filter negate proto

Inverse protocol.

```
diagnose sys mcast-session filter negate proto
```

diagnose sys mcast-session filter negate intf

Inverse source interface.

```
diagnose sys mcast-session filter negate intf
```

diagnose sys mcast-session filter negate sport

Inverse source port.

```
diagnose sys mcast-session filter negate sport
```

diagnose sys mcast-session filter negate src

Inverse source IP.

```
diagnose sys mcast-session filter negate src
```

diagnose sys mcast-session filter negate vd

Inverse virtual domain.

```
diagnose sys mcast-session filter negate vd
```

diagnose sys mcast-session filter proto

Protocol number.

```
diagnose sys mcast-session filter proto <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255> (from).	string	
<xx>	<0-255> (to).	string	

diagnose sys mcast-session filter intf

Source interface.

```
diagnose sys mcast-session filter intf <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	Interface name.	string	

diagnose sys mcast-session filter sport

Source port.

```
diagnose sys mcast-session filter sport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys mcast-session filter src

Source IP address.


```
diagnose sys mcast-session filter src <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (from).	string	
<xxx.xxx.xxx.xxx>	Source IP (to).	string	

diagnose sys mcast-session filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys mcast-session filter vd <xxx>
```

Parameter	Description	Type	Size
<xxx>	Index of virtual domain. -1 matches all.	string	

diagnose sys mcast-session list

List session.

```
diagnose sys mcast-session list
```

diagnose sys mcast-session stat

Stat session.

```
diagnose sys mcast-session stat
```

diagnose sys mcast-session6

IPv6 multicast session.

```
diagnose sys mcast-session6
```

diagnose sys mcast-session6 clear

Clear IPv6 multicast sessions defined by filter.

```
diagnose sys mcast-session6 clear
```

diagnose sys mcast-session6 filter

List IPv6 multicast session with filters.

```
diagnose sys mcast-session6 filter
```

diagnose sys mcast-session6 filter clear

Clear IPv6 multicast session filter.

```
diagnose sys mcast-session6 filter clear
```

diagnose sys mcast-session6 filter clear dport

Clear destination port filter.

```
diagnose sys mcast-session6 filter clear dport
```

diagnose sys mcast-session6 filter clear dst

Clear destination IP filter.

```
diagnose sys mcast-session6 filter clear dst
```

diagnose sys mcast-session6 filter clear proto

Clear protocol filter.

```
diagnose sys mcast-session6 filter clear proto
```

diagnose sys mcast-session6 filter clear intf

Clear source interface filter.

```
diagnose sys mcast-session6 filter clear intf
```

diagnose sys mcast-session6 filter clear sport

Clear source port filter.

```
diagnose sys mcast-session6 filter clear sport
```

diagnose sys mcast-session6 filter clear src

Clear source IP filter.

```
diagnose sys mcast-session6 filter clear src
```

diagnose sys mcast-session6 filter clear vd

Clear virtual domain filter.

```
diagnose sys mcast-session6 filter clear vd
```

diagnose sys mcast-session6 filter dport

Destination port.

```
diagnose sys mcast-session6 filter dport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys mcast-session6 filter dst

Destination IP address.

```
diagnose sys mcast-session6 filter dst <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP (from).	string	
<xxx.xxx.xxx.xxx>	Destination IP (to).	string	

diagnose sys mcast-session6 filter negate

Inverse filter.

```
diagnose sys mcast-session6 filter negate
```

diagnose sys mcast-session6 filter negate dport

Inverse destination port.

```
diagnose sys mcast-session6 filter negate dport
```

diagnose sys mcast-session6 filter negate dst

Inverse destination IP.

```
diagnose sys mcast-session6 filter negate dst
```

diagnose sys mcast-session6 filter negate proto

Inverse protocol.

```
diagnose sys mcast-session6 filter negate proto
```

diagnose sys mcast-session6 filter negate intf

Inverse source interface.

```
diagnose sys mcast-session6 filter negate intf
```

diagnose sys mcast-session6 filter negate sport

Inverse source port.

```
diagnose sys mcast-session6 filter negate sport
```

diagnose sys mcast-session6 filter negate src

Inverse source IP.

```
diagnose sys mcast-session6 filter negate src
```

diagnose sys mcast-session6 filter negate vd

Inverse virtual domain.

```
diagnose sys mcast-session6 filter negate vd
```

diagnose sys mcast-session6 filter proto

Protocol number.

```
diagnose sys mcast-session6 filter proto <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255> (from).	string	
<xx>	<0-255> (to).	string	

diagnose sys mcast-session6 filter intf

Source interface.

```
diagnose sys mcast-session6 filter intf <xxxxx>
```

Parameter	Description	Type	Size
<xxxxx>	Interface name.	string	

diagnose sys mcast-session6 filter sport

Source port.

```
diagnose sys mcast-session6 filter sport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys mcast-session6 filter src

Source IP address.

```
diagnose sys mcast-session6 filter src <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (from).	string	
<xxx.xxx.xxx.xxx>	Source IP (to).	string	

diagnose sys mcast-session6 filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys mcast-session6 filter vd <xxx>
```

Parameter	Description	Type	Size
<xxx>	Index of virtual domain. -1 matches all.	string	

diagnose sys mcast-session6 list

List IPv6 multicast session.

```
diagnose sys mcast-session6 list
```

diagnose sys mcast-session6 stat

Stat IPv6 multicast session.

```
diagnose sys mcast-session6 stat
```

diagnose sys mpstat

mpstat

```
diagnose sys mpstat <value> <value>
```

Parameter	Description	Type	Size
<value>	Delay in seconds (default 5).	string	
<value>	Loop times (default = 1,000,000).	string	

diagnose sys ntp

NTP daemon command.

```
diagnose sys ntp
```

diagnose sys ntp status

List NTP servers information.

```
diagnose sys ntp status
```

diagnose sys pair

Pair device.

```
diagnose sys pair
```

diagnose sys platform

Platform information.

```
diagnose sys platform
```

diagnose sys platform info

Information.

```
diagnose sys platform info
```

diagnose sys print-conserve-info

Print all conserve related info.

```
diagnose sys print-conserve-info
```

diagnose sys process

Dump process stack.

```
diagnose sys process
```

diagnose sys process daemon-auto-restart

Set daemon respawn behaviour.

```
diagnose sys process daemon-auto-restart <action> <daemon>
```

Parameter	Description	Type	Size
<action>	(enable disable)	string	
<daemon>	Daemon name.	string	

diagnose sys process dump

Dump process kernel stack.

```
diagnose sys process dump <pid>
```

Parameter	Description	Type	Size
<pid>	PID of the process to dump.	string	

diagnose sys process nameof

List name of process with a specific PID.

```
diagnose sys process nameof <integer>
```

Parameter	Description	Type	Size
<integer>	PID to find the process name.	string	

diagnose sys process pidof

List PIDs of processes with a specific name.

```
diagnose sys process pidof <string>
```

Parameter	Description	Type	Size
<string>	Name to find PIDs for.	string	

diagnose sys process pstack

Dump process userspace stack.

```
diagnose sys process pstack <pid>
```

Parameter	Description	Type	Size
<pid>	PID of the process to dump.	string	

diagnose sys process sock-mem

Show process socket mem usage.

```
diagnose sys process sock-mem
```

diagnose sys process socket

Find PID of processes which owns the socket.

```
diagnose sys process socket <socket-inode>
```

Parameter	Description	Type	Size
<socket-inode>	Socket to find PID for.	string	

diagnose sys process trace

Sample process instructions.

```
diagnose sys process trace
```

diagnose sys profile

kernel profiling

```
diagnose sys profile
```

diagnose sys profile cpumask

profile which CPUs

```
diagnose sys profile cpumask
```

diagnose sys profile module

show kernel module

```
diagnose sys profile module
```

diagnose sys profile show

show kernel profiling result

```
diagnose sys profile show
```

diagnose sys profile show detail

show detail of kernel profiling

```
diagnose sys profile show detail
```

diagnose sys profile show order

order kernel profiling result

```
diagnose sys profile show order
```

diagnose sys profile start

start kernel profiling data

```
diagnose sys profile start
```

diagnose sys profile step

set profile step

```
diagnose sys profile step <Integer>
```

Parameter	Description	Type	Size
<Integer>	Profile step for CPU profiling. Argument should be a power of two between 2 to 32	string	

diagnose sys profile stop

copy kernel profiling data

```
diagnose sys profile stop
```

diagnose sys profile sysmap

show kernel sysmap

```
diagnose sys profile sysmap
```

diagnose sys proxy

Proxy diagnostics.

```
diagnose sys proxy
```

diagnose sys proxy bypass

Bypass setting.

```
diagnose sys proxy bypass
```

diagnose sys proxy bypass clear

Clear bypass settings.

```
diagnose sys proxy bypass clear
```

diagnose sys proxy bypass disable

Disable bypass settings.

```
diagnose sys proxy bypass disable
```

diagnose sys proxy bypass disable category

Disable category bypass.

```
diagnose sys proxy bypass disable category
```

diagnose sys proxy bypass disable category all

Bypass all.

```
diagnose sys proxy bypass disable category all
```

diagnose sys proxy bypass disable category scanunit-submission

Bypass scanunit submission.

```
diagnose sys proxy bypass disable category scanunit-submission
```

diagnose sys proxy bypass disable category ssl

Bypass SSL (no crypto, no utm).

```
diagnose sys proxy bypass disable category ssl
```

diagnose sys proxy bypass disable category utm

Bypass UTM (crypto, no utm).

```
diagnose sys proxy bypass disable category utm
```

diagnose sys proxy bypass disable protocol

Disable protocol bypass.

```
diagnose sys proxy bypass disable protocol
```

diagnose sys proxy bypass disable protocol all

All proxy protocols

```
diagnose sys proxy bypass disable protocol all
```

diagnose sys proxy bypass disable protocol ftp

FTP(S) protocol

```
diagnose sys proxy bypass disable protocol ftp
```

diagnose sys proxy bypass disable protocol imap

IMAP(S) protocol

```
diagnose sys proxy bypass disable protocol imap
```

diagnose sys proxy bypass disable protocol nntp

NNTP protocol

```
diagnose sys proxy bypass disable protocol nntp
```

diagnose sys proxy bypass disable protocol pop3

POP3(S) protocol

```
diagnose sys proxy bypass disable protocol pop3
```

diagnose sys proxy bypass disable protocol smtp

SMTP(S) protocol

```
diagnose sys proxy bypass disable protocol smtp
```

diagnose sys proxy bypass enable

Enable bypass settings.

```
diagnose sys proxy bypass enable
```

diagnose sys proxy bypass enable category

Enable category bypass.

```
diagnose sys proxy bypass enable category
```

diagnose sys proxy bypass enable category all

Bypass all.

```
diagnose sys proxy bypass enable category all
```

diagnose sys proxy bypass enable category scanunit-submission

Bypass scanunit submission.

```
diagnose sys proxy bypass enable category scanunit-submission
```

diagnose sys proxy bypass enable category ssl

Bypass SSL (no crypto, no utm).

```
diagnose sys proxy bypass enable category ssl
```

diagnose sys proxy bypass enable category utm

Bypass UTM (crypto, no utm).

```
diagnose sys proxy bypass enable category utm
```

diagnose sys proxy bypass enable protocol

Enable protocol bypass.

```
diagnose sys proxy bypass enable protocol
```

diagnose sys proxy bypass enable protocol all

All proxy protocols

```
diagnose sys proxy bypass enable protocol all
```

diagnose sys proxy bypass enable protocol ftp

FTP(S) protocol

```
diagnose sys proxy bypass enable protocol ftp
```

diagnose sys proxy bypass enable protocol imap

IMAP(S) protocol

```
diagnose sys proxy bypass enable protocol imap
```

diagnose sys proxy bypass enable protocol nntp

NNTP protocol

```
diagnose sys proxy bypass enable protocol nntp
```

diagnose sys proxy bypass enable protocol pop3

POP3(S) protocol

```
diagnose sys proxy bypass enable protocol pop3
```

diagnose sys proxy bypass enable protocol smtp

SMTP(S) protocol

```
diagnose sys proxy bypass enable protocol smtp
```

diagnose sys proxy bypass show

Show bypass settings.

```
diagnose sys proxy bypass show
```

diagnose sys proxy certificate-blocklist

Certificate blocklist diagnostics.

```
diagnose sys proxy certificate-blocklist
```

diagnose sys proxy certificate-blocklist flush

Flush certificate blocklist database.

```
diagnose sys proxy certificate-blocklist flush
```


diagnose sys proxy certificate-blocklist status

Display per worker certificate blocklist status.

```
diagnose sys proxy certificate-blocklist status
```

diagnose sys proxy debug-filter

Filter for displaying debug information.

```
diagnose sys proxy debug-filter
```

diagnose sys proxy debug-filter clear

Erase the current filter.

```
diagnose sys proxy debug-filter clear
```

diagnose sys proxy debug-filter list

Display the current filter.

```
diagnose sys proxy debug-filter list
```

diagnose sys proxy debug-filter src

Source address range to filter by.

```
diagnose sys proxy debug-filter src <ip-address> <ip-address>
```

Parameter	Description	Type	Size
<ip-address>	Source IP address (from).	string	
<ip-address>	Source IP address (to).	string	

diagnose sys proxy filter

Diagnostics filter.

```
diagnose sys proxy filter
```

diagnose sys proxy filter clear

Clear the current filter.

```
diagnose sys proxy filter clear
```

diagnose sys proxy filter list

Display the current filter.

```
diagnose sys proxy filter list
```

diagnose sys proxy filter negate

Negate the specified filter parameter.

```
diagnose sys proxy filter negate
```

diagnose sys proxy filter negate vd

Negate virtual domain.

```
diagnose sys proxy filter negate vd
```

diagnose sys proxy filter negate worker

Negate worker ID.

```
diagnose sys proxy filter negate worker
```

diagnose sys proxy filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys proxy filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose sys proxy filter worker

ID of worker or "m" for manager. Invalid ID matches all.

```
diagnose sys proxy filter worker <id>
```

Parameter	Description	Type	Size
<id>	ID of worker or "m" for manager. Invalid ID matches all.	string	

diagnose sys proxy log

Logging diagnostics.

```
diagnose sys proxy log
```

diagnose sys proxy log filter

Debug log filter.

```
diagnose sys proxy log filter
```

diagnose sys proxy log filter clear

Clear the current filter.

```
diagnose sys proxy log filter clear
```

diagnose sys proxy log filter list

Display the current filter.

```
diagnose sys proxy log filter list
```

diagnose sys proxy log filter negate

Negate the specified filter parameter.

```
diagnose sys proxy log filter negate
```

diagnose sys proxy log filter negate vd

Negate virtual domain.

```
diagnose sys proxy log filter negate vd
```

diagnose sys proxy log filter negate worker

Negate worker ID.

```
diagnose sys proxy log filter negate worker
```

diagnose sys proxy log filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys proxy log filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose sys proxy log filter worker

ID of worker or "m" for manager. Invalid ID matches all.

```
diagnose sys proxy log filter worker <id>
```

Parameter	Description	Type	Size
<id>	ID of worker or "m" for manager. Invalid ID matches all.	string	

diagnose sys proxy log-debug

Enable/disable sys proxy log on console.

```
diagnose sys proxy log-debug <integer>
```

Parameter	Description	Type	Size
<integer>	Enable/disable log on console, 0 off, otherwise, on.	string	

diagnose sys proxy memory

Memory configuration

```
diagnose sys proxy memory
```

diagnose sys proxy memory allocator

Show the current memory allocator

```
diagnose sys proxy memory allocator
```

diagnose sys proxy memory conserve

Enter/exit conserve mode.

```
diagnose sys proxy memory conserve
```

diagnose sys proxy memory conserve enter

Enter conserve mode.

```
diagnose sys proxy memory conserve enter
```

diagnose sys proxy memory conserve exit

Exit conserve mode.

```
diagnose sys proxy memory conserve exit
```

diagnose sys proxy memory jemalloc

Use jemalloc for memory allocation

```
diagnose sys proxy memory jemalloc
```

diagnose sys proxy memory malloc

Use malloc for memory allocation

```
diagnose sys proxy memory malloc
```

diagnose sys proxy memory usage

Per-worker memory allocation statistics

```
diagnose sys proxy memory usage
```

diagnose sys proxy restart

Restart proxy.

```
diagnose sys proxy restart
```

diagnose sys proxy simulate-error

Error test options.

```
diagnose sys proxy simulate-error
```

diagnose sys proxy simulate-error scan-drop

Enable/disable proxy error scan drop.

```
diagnose sys proxy simulate-error scan-drop
```

diagnose sys proxy simulate-error scan-drop disable

Disable scan-drop (default)

```
diagnose sys proxy simulate-error scan-drop disable
```

diagnose sys proxy simulate-error scan-drop enable

Enable scan-drop

```
diagnose sys proxy simulate-error scan-drop enable
```

diagnose sys proxy simulate-error status

Display per worker error test options.

```
diagnose sys proxy simulate-error status
```

diagnose sys proxy socket-options

Socket options configuration

```
diagnose sys proxy socket-options
```

diagnose sys proxy socket-options linger

SO_LINGER socket option

```
diagnose sys proxy socket-options linger
```

diagnose sys proxy socket-options linger disable

Disable SO_LINGER

```
diagnose sys proxy socket-options linger disable
```

diagnose sys proxy socket-options linger enable

Enable SO_LINGER

```
diagnose sys proxy socket-options linger enable
```

diagnose sys proxy socket-options nagle

SSL TCP_NODELAY socket option

```
diagnose sys proxy socket-options nagle
```

diagnose sys proxy socket-options nagle disable

Disable TCP_NODELAY for SSL connections (Default)

```
diagnose sys proxy socket-options nagle disable
```

diagnose sys proxy socket-options nagle enable

Enable TCP_NODELAY for SSL connections

```
diagnose sys proxy socket-options nagle enable
```

diagnose sys proxy socket-options status

Display per worker socket options

```
diagnose sys proxy socket-options status
```

diagnose sys proxy ssl

SSL options

```
diagnose sys proxy ssl
```

diagnose sys proxy ssl bypass

Ssl bypass cache

```
diagnose sys proxy ssl bypass
```


diagnose sys proxy ssl bypass flush

Flush ssl bypass cache

```
diagnose sys proxy ssl bypass flush
```

diagnose sys proxy ssl bypass list

List ssl bypass cache

```
diagnose sys proxy ssl bypass list
```

diagnose sys proxy ssl crypto

Set hardware crypto mode

```
diagnose sys proxy ssl crypto
```

diagnose sys proxy ssl crypto async

Asynchronous hardware crypto

```
diagnose sys proxy ssl crypto async
```

diagnose sys proxy ssl crypto sync

Synchronous hardware crypto

```
diagnose sys proxy ssl crypto sync
```

diagnose sys proxy ssl exempt

Ssl exempt cache

```
diagnose sys proxy ssl exempt
```

diagnose sys proxy ssl exempt flush

Flush ssl exempt cache

```
diagnose sys proxy ssl exempt flush
```

diagnose sys proxy ssl exempt list

List ssl exempt cache

```
diagnose sys proxy ssl exempt list
```

diagnose sys proxy ssl rsa-blinding

Set RSA blinding

```
diagnose sys proxy ssl rsa-blinding
```

diagnose sys proxy ssl rsa-blinding off

RSA blinding off

```
diagnose sys proxy ssl rsa-blinding off
```

diagnose sys proxy ssl rsa-blinding on

RSA blinding on

```
diagnose sys proxy ssl rsa-blinding on
```

diagnose sys proxy ssl session

List of current SSL sessions

```
diagnose sys proxy ssl session
```

diagnose sys proxy stats

Proxy statistics.

```
diagnose sys proxy stats
```

diagnose sys proxy stats all

Per-process proxy statistics.

```
diagnose sys proxy stats all
```

diagnose sys proxy stats clear

Clear proxy statistics.

```
diagnose sys proxy stats clear
```

diagnose sys proxy stats debug

Debug sink statistics

```
diagnose sys proxy stats debug
```

diagnose sys proxy stats list

Summarized proxy statistics.

```
diagnose sys proxy stats list
```

diagnose sys proxy stats protocol

Per-process proxy worker protocol statistics.

```
diagnose sys proxy stats protocol
```

diagnose sys proxy stats vdom

Proxy vdom statistics.

```
diagnose sys proxy stats vdom
```

diagnose sys proxy stats vdom all

Proxy per-vdom statistics.

```
diagnose sys proxy stats vdom all
```

diagnose sys proxy stats vdom list

List current vdoms.

```
diagnose sys proxy stats vdom list
```

diagnose sys proxy stats vdom summary

Summarized vdom proxy statistics.

```
diagnose sys proxy stats vdom summary
```

diagnose sys proxy valgrind

Valgrind analysis.

```
diagnose sys proxy valgrind
```

diagnose sys proxy valgrind disable

Force daemon to restart.

```
diagnose sys proxy valgrind disable
```

diagnose sys proxy valgrind enable

Force daemon to restart.

```
diagnose sys proxy valgrind enable
```

diagnose sys proxy valgrind log

Valgrind logs.

```
diagnose sys proxy valgrind log
```

diagnose sys proxy valgrind log clear

Clear logs.

```
diagnose sys proxy valgrind log clear
```

diagnose sys proxy valgrind log show

Show logs.

```
diagnose sys proxy valgrind log show
```

diagnose sys proxy valgrind memcheck

Force daemon to restart.

```
diagnose sys proxy valgrind memcheck
```

diagnose sys proxy valgrind memcheck_less

Force daemon to restart.

```
diagnose sys proxy valgrind memcheck_less
```

diagnose sys proxy valgrind status

Show valgrind status.

```
diagnose sys proxy valgrind status
```

diagnose sys ptp

PTP daemon command.

```
diagnose sys ptp
```

diagnose sys ptp status

List PTP information.

```
diagnose sys ptp status
```

diagnose sys route_tag

route-tag.

```
diagnose sys route_tag
```

diagnose sys route_tag flush

Flush route tag address.

```
diagnose sys route_tag flush <route-tag>
```

Parameter	Description	Type	Size
<route-tag>	Flush cache of route-tag address in SD-WAN.	string	

diagnose sys route_tag list

Show route tag address.

```
diagnose sys route_tag list <route-tag>
```

Parameter	Description	Type	Size
<route-tag>	Show details of route-tag address.	string	

diagnose sys route_tag summary

route tag address summary.

```
diagnose sys route_tag summary
```

diagnose sys saml

SAML diagnostics.

```
diagnose sys saml
```

diagnose sys saml metadata

Test metadata.

```
diagnose sys saml metadata
```

diagnose sys scanunit

Scanunit diagnostics.

```
diagnose sys scanunit
```

diagnose sys scanunit auto-restart

Auto-restart settings.

```
diagnose sys scanunit auto-restart
```

diagnose sys scanunit auto-restart requests

Number of scan requests before restarting.

```
diagnose sys scanunit auto-restart requests <Integer>
```

Parameter	Description	Type	Size
<Integer>	Number of requests before restarting (0 disables auto restart).	string	

diagnose sys scanunit auto-restart reset

Reset auto restart settings.

```
diagnose sys scanunit auto-restart reset
```

diagnose sys scanunit auto-restart status

Show auto restart settings.

```
diagnose sys scanunit auto-restart status
```

diagnose sys scanunit auto-restart time

Minimum interval in seconds between restarting workers.

```
diagnose sys scanunit auto-restart time <Integer>
```

Parameter	Description	Type	Size
<Integer>	Minimum interval in seconds between restarting workers.	string	

diagnose sys scanunit av

Configure scanunit av settings.

```
diagnose sys scanunit av
```

diagnose sys scanunit av filetype-reuse

Enable/disable AV filetype reuse.

```
diagnose sys scanunit av filetype-reuse
```


diagnose sys scanunit av filetype-reuse disable

Disable scanunit AV filetype reuse.

```
diagnose sys scanunit av filetype-reuse disable
```

diagnose sys scanunit av filetype-reuse enable

Enable scanunit AV filetype reuse.

```
diagnose sys scanunit av filetype-reuse enable
```

diagnose sys scanunit av reload-avdb

Reload AVDB.

```
diagnose sys scanunit av reload-avdb
```

diagnose sys scanunit av reload-aveng

Reload AV engine.

```
diagnose sys scanunit av reload-aveng
```

diagnose sys scanunit av reload-fsa-ext

Reload FSA extensions list.

```
diagnose sys scanunit av reload-fsa-ext
```

diagnose sys scanunit bypass

Bypass setting.

```
diagnose sys scanunit bypass
```

diagnose sys scanunit bypass clear

Clear bypass settings.

```
diagnose sys scanunit bypass clear
```

diagnose sys scanunit bypass disable

Disable bypass settings.

```
diagnose sys scanunit bypass disable
```

diagnose sys scanunit bypass disable category

Disable category bypass.

```
diagnose sys scanunit bypass disable category
```

diagnose sys scanunit bypass disable category all

Bypass all.

```
diagnose sys scanunit bypass disable category all
```

diagnose sys scanunit bypass disable category av-engine

Bypass AV engine.

```
diagnose sys scanunit bypass disable category av-engine
```

diagnose sys scanunit bypass disable category scanunit

Bypass scanunit.

```
diagnose sys scanunit bypass disable category scanunit
```

diagnose sys scanunit bypass disable protocol

Disable protocol bypass.

```
diagnose sys scanunit bypass disable protocol
```

diagnose sys scanunit bypass disable protocol all

All proxy protocols

```
diagnose sys scanunit bypass disable protocol all
```

diagnose sys scanunit bypass disable protocol cifs

CIFS protocol

```
diagnose sys scanunit bypass disable protocol cifs
```

diagnose sys scanunit bypass disable protocol ftp

FTP(S) protocol

```
diagnose sys scanunit bypass disable protocol ftp
```

diagnose sys scanunit bypass disable protocol http

HTTP(S) protocol

```
diagnose sys scanunit bypass disable protocol http
```

diagnose sys scanunit bypass disable protocol imap

IMAP(S) protocol

```
diagnose sys scanunit bypass disable protocol imap
```

diagnose sys scanunit bypass disable protocol nntp

NNTP protocol

```
diagnose sys scanunit bypass disable protocol nntp
```

diagnose sys scanunit bypass disable protocol pop3

POP3(S) protocol

```
diagnose sys scanunit bypass disable protocol pop3
```

diagnose sys scanunit bypass disable protocol smtp

SMTP(S) protocol

```
diagnose sys scanunit bypass disable protocol smtp
```

diagnose sys scanunit bypass enable

Enable bypass settings.

```
diagnose sys scanunit bypass enable
```

diagnose sys scanunit bypass enable category

Enable category bypass.

```
diagnose sys scanunit bypass enable category
```

diagnose sys scanunit bypass enable category all

Bypass all.

```
diagnose sys scanunit bypass enable category all
```

diagnose sys scanunit bypass enable category av-engine

Bypass AV engine.

```
diagnose sys scanunit bypass enable category av-engine
```

diagnose sys scanunit bypass enable category scanunit

Bypass scanunit.

```
diagnose sys scanunit bypass enable category scanunit
```

diagnose sys scanunit bypass enable protocol

Enable protocol bypass.

```
diagnose sys scanunit bypass enable protocol
```

diagnose sys scanunit bypass enable protocol all

All proxy protocols

```
diagnose sys scanunit bypass enable protocol all
```

diagnose sys scanunit bypass enable protocol cifs

CIFS protocol

```
diagnose sys scanunit bypass enable protocol cifs
```

diagnose sys scanunit bypass enable protocol ftp

FTP(S) protocol

```
diagnose sys scanunit bypass enable protocol ftp
```

diagnose sys scanunit bypass enable protocol http

HTTP(S) protocol

```
diagnose sys scanunit bypass enable protocol http
```

diagnose sys scanunit bypass enable protocol imap

IMAP(S) protocol

```
diagnose sys scanunit bypass enable protocol imap
```

diagnose sys scanunit bypass enable protocol nntp

NNTP protocol

```
diagnose sys scanunit bypass enable protocol nntp
```

diagnose sys scanunit bypass enable protocol pop3

POP3(S) protocol

```
diagnose sys scanunit bypass enable protocol pop3
```

diagnose sys scanunit bypass enable protocol smtp

SMTP(S) protocol

```
diagnose sys scanunit bypass enable protocol smtp
```

diagnose sys scanunit bypass show

Show bypass settings.

```
diagnose sys scanunit bypass show
```

diagnose sys scanunit cfg

Cached configuration.

```
diagnose sys scanunit cfg
```

diagnose sys scanunit cfg clear

Clear cached configuration.

```
diagnose sys scanunit cfg clear
```

diagnose sys scanunit cfg list

List the key for each cached configuration entry.

```
diagnose sys scanunit cfg list
```

diagnose sys scanunit crash-dump

Enable/disable crash dump.

```
diagnose sys scanunit crash-dump
```

diagnose sys scanunit crash-dump clear

Clear scanunit crash dump.

```
diagnose sys scanunit crash-dump clear
```

diagnose sys scanunit crash-dump disable

Disable scanunit crash dump.

```
diagnose sys scanunit crash-dump disable
```

diagnose sys scanunit crash-dump enable

Enable scanunit crash dump.

```
diagnose sys scanunit crash-dump enable
```

diagnose sys scanunit crash-dump read

Read the last crash dump.

```
diagnose sys scanunit crash-dump read
```

diagnose sys scanunit debug

Debug settings.

```
diagnose sys scanunit debug
```

diagnose sys scanunit debug all

Enable all debug categories.

```
diagnose sys scanunit debug all <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug analytics

Enable analytics category.

```
diagnose sys scanunit debug analytics <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug antispam

Enable antispam category.

```
diagnose sys scanunit debug antispam <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug daemon

Enable scanunit daemon category.

```
diagnose sys scanunit debug daemon <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug dlp

Enable DLP category.

```
diagnose sys scanunit debug dlp <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug fhl

Enable FHL category.

```
diagnose sys scanunit debug fhl <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug file-filter

Enable file filter category.

```
diagnose sys scanunit debug file-filter <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug icb

Enable ICB category.

```
diagnose sys scanunit debug icb <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug job

Enable scanunit job category.

```
diagnose sys scanunit debug job <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug level

Set debug level.

```
diagnose sys scanunit debug level
```

diagnose sys scanunit debug level error

Error level.

```
diagnose sys scanunit debug level error
```

diagnose sys scanunit debug level info

Info level.

```
diagnose sys scanunit debug level info
```

diagnose sys scanunit debug level verbose

Verbose level.

```
diagnose sys scanunit debug level verbose
```

diagnose sys scanunit debug level warning

Warning level.

```
diagnose sys scanunit debug level warning
```

diagnose sys scanunit debug outbreak-prevention

Enable outbreak prevention category.

```
diagnose sys scanunit debug outbreak-prevention <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug quarantine

Enable quarantine category.

```
diagnose sys scanunit debug quarantine <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug reset

Reset debug category and level.

```
diagnose sys scanunit debug reset
```

diagnose sys scanunit debug sane

Enable a sane group of categories.

```
diagnose sys scanunit debug sane <status>
```

Parameter	Description	Type	Size
<status>	Enable or disable debug category.	string	

diagnose sys scanunit debug show

Show current debug settings.

```
diagnose sys scanunit debug show
```

diagnose sys scanunit debug start

Force start scanunit debug connection.

```
diagnose sys scanunit debug start
```

diagnose sys scanunit debug stop

Force stop scanunit debug connection.

```
diagnose sys scanunit debug stop
```

diagnose sys scanunit dlp

DLP data size scanning threshold settings.

```
diagnose sys scanunit dlp
```

diagnose sys scanunit dlp config

Commands for building the dlp config.

```
diagnose sys scanunit dlp config
```

diagnose sys scanunit dlp config build

Rebuild the dlp config.

```
diagnose sys scanunit dlp config build
```

diagnose sys scanunit dlp config status

Show the current status of the dlp builder.

```
diagnose sys scanunit dlp config status
```

diagnose sys scanunit dlp config term

Terminate the dlp config builder process, if running.

```
diagnose sys scanunit dlp config term
```

diagnose sys scanunit dlp reset

Reset DLP data size scanning threshold value.

```
diagnose sys scanunit dlp reset
```

diagnose sys scanunit dlp status

Show DLP data size scanning threshold value.

```
diagnose sys scanunit dlp status
```

diagnose sys scanunit dlp threshold

Set DLP data size scanning threshold in bytes (0 = default).

```
diagnose sys scanunit dlp threshold <Integer>
```

Parameter	Description	Type	Size
<Integer>	DLP data size scanning threshold.	string	

diagnose sys scanunit file-hash

File hash list.

```
diagnose sys scanunit file-hash
```

diagnose sys scanunit file-hash list

List malware hashes.

```
diagnose sys scanunit file-hash list
```

diagnose sys scanunit file-hash list all

List all malware hashes.

```
diagnose sys scanunit file-hash list all
```

diagnose sys scanunit file-hash list md5

List md5 malware hashes.

```
diagnose sys scanunit file-hash list md5
```

diagnose sys scanunit file-hash list sha1

List sha1 malware hashes.

```
diagnose sys scanunit file-hash list sha1
```

diagnose sys scanunit file-hash list sha256

List sha256 malware hashes.

```
diagnose sys scanunit file-hash list sha256
```

diagnose sys scanunit file-hash query

Query a malware hash.

```
diagnose sys scanunit file-hash query
```

diagnose sys scanunit file-hash query md5

Query an md5 malware hash.

```
diagnose sys scanunit file-hash query md5 <value>
```

Parameter	Description	Type	Size
<value>	md5 hash	string	

diagnose sys scanunit file-hash query sha1

Query a sha1 malware hash.

```
diagnose sys scanunit file-hash query sha1 <value>
```

Parameter	Description	Type	Size
<value>	sha1 hash	string	

diagnose sys scanunit file-hash query sha256

Query a sha256 malware hash.

```
diagnose sys scanunit file-hash query sha256 <value>
```

Parameter	Description	Type	Size
<value>	sha256 hash	string	

diagnose sys scanunit file-hash status

File hash database status.

```
diagnose sys scanunit file-hash status
```

diagnose sys scanunit filter

Diagnostics filter.

```
diagnose sys scanunit filter
```

diagnose sys scanunit filter clear

Clear the current filter.

```
diagnose sys scanunit filter clear
```

diagnose sys scanunit filter list

Display the current filter.

```
diagnose sys scanunit filter list
```

diagnose sys scanunit filter negate

Negate the specified filter parameter.

```
diagnose sys scanunit filter negate
```

diagnose sys scanunit filter negate vd

Negate virtual domain.

```
diagnose sys scanunit filter negate vd
```

diagnose sys scanunit filter negate worker

Negate worker ID.

```
diagnose sys scanunit filter negate worker
```


diagnose sys scanunit filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys scanunit filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose sys scanunit filter worker

ID of worker or "m" for manager. Invalid ID matches all.

```
diagnose sys scanunit filter worker <id>
```

Parameter	Description	Type	Size
<id>	ID of worker or "m" for manager. Invalid ID matches all.	string	

diagnose sys scanunit info

Scanunit process info.

```
diagnose sys scanunit info
```

diagnose sys scanunit info shared_status

Print contents of shared status.

```
diagnose sys scanunit info shared_status
```

diagnose sys scanunit log

Logging diagnostics.

```
diagnose sys scanunit log
```

diagnose sys scanunit log filter

Debug log filter.

```
diagnose sys scanunit log filter
```

diagnose sys scanunit log filter clear

Clear the current filter.

```
diagnose sys scanunit log filter clear
```

diagnose sys scanunit log filter list

Display the current filter.

```
diagnose sys scanunit log filter list
```

diagnose sys scanunit log filter negate

Negate the specified filter parameter.

```
diagnose sys scanunit log filter negate
```

diagnose sys scanunit log filter negate vd

Negate virtual domain.

```
diagnose sys scanunit log filter negate vd
```

diagnose sys scanunit log filter negate worker

Negate worker ID.

```
diagnose sys scanunit log filter negate worker
```

diagnose sys scanunit log filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys scanunit log filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose sys scanunit log filter worker

ID of worker or "m" for manager. Invalid ID matches all.

```
diagnose sys scanunit log filter worker <id>
```

Parameter	Description	Type	Size
<id>	ID of worker or "m" for manager. Invalid ID matches all.	string	

diagnose sys scanunit memory

Memory configuration

```
diagnose sys scanunit memory
```

diagnose sys scanunit memory conserve

Enter/exit conserve mode.

```
diagnose sys scanunit memory conserve
```

diagnose sys scanunit memory conserve enter

Enter conserve mode.

```
diagnose sys scanunit memory conserve enter
```

diagnose sys scanunit memory conserve exit

Exit conserve mode.

```
diagnose sys scanunit memory conserve exit
```

diagnose sys scanunit restart

Restart scanunit.

```
diagnose sys scanunit restart <which>
```

Parameter	Description	Type	Size
<which>	Worker id to restart. Or 'all' for all processes.	string	

diagnose sys scanunit simulate-crash

Simulate scanunit crashes.

```
diagnose sys scanunit simulate-crash
```

diagnose sys scanunit simulate-crash lockup-workers

Simulate locked up scanunit workers.

```
diagnose sys scanunit simulate-crash lockup-workers
```

diagnose sys scanunit simulate-crash lockup-workers all

Lock up all workers.

```
diagnose sys scanunit simulate-crash lockup-workers all
```

diagnose sys scanunit simulate-crash lockup-workers worker

Lock up worker <id>.

```
diagnose sys scanunit simulate-crash lockup-workers worker <id>
```

Parameter	Description	Type	Size
<id>	ID of worker to lock up.	string	

diagnose sys scanunit simulate-error

Simulate scanunit errors.

```
diagnose sys scanunit simulate-error
```

diagnose sys scanunit simulate-error av-engine-delay

Add delay in AV engine filetype callback

```
diagnose sys scanunit simulate-error av-engine-delay <Integer>
```

Parameter	Description	Type	Size
<Integer>	Delay (in seconds) to introduce in AV engine filetype callback	string	

diagnose sys scanunit simulate-error av-error

Simulate AV engine error codes

```
diagnose sys scanunit simulate-error av-error <Integer>
```

Parameter	Description	Type	Size
<Integer>	AV engine error code, interpreted as bitmask.	string	

diagnose sys scanunit simulate-error av-status

Simulate AV engine status codes.

```
diagnose sys scanunit simulate-error av-status <Integer>
```

Parameter	Description	Type	Size
<Integer>	AV engine status code. (-1 == INFECTED_ERROR, 1 == INFECTED_VIRUS, etc.)	string	

diagnose sys scanunit simulate-error cdr-error

Simulate CDR engine internal error when active content detected.

```
diagnose sys scanunit simulate-error cdr-error
```

diagnose sys scanunit simulate-error reset

Reset all error simulation settings.

```
diagnose sys scanunit simulate-error reset
```

diagnose sys scanunit simulate-error scan-error-code

Simulate scanunit scan error.

```
diagnose sys scanunit simulate-error scan-error-code <Integer>
```

Parameter	Description	Type	Size
<Integer>	Scanunit error code (negated) (e.g., 0 = none, 3 = invalid infection pointer, 5 = scanunit crash).	string	

diagnose sys scanunit simulate-error status

Show error simulation settings.

```
diagnose sys scanunit simulate-error status
```

diagnose sys scanunit stats

Statistics.

```
diagnose sys scanunit stats
```

diagnose sys scanunit stats all

Per-process statistics.

```
diagnose sys scanunit stats all
```

diagnose sys scanunit stats builder

scanunit builder statistics.

```
diagnose sys scanunit stats builder
```

diagnose sys scanunit stats clear

Clear all statistics.

```
diagnose sys scanunit stats clear
```

diagnose sys scanunit stats crash

Crash process statistics.

```
diagnose sys scanunit stats crash
```

diagnose sys scanunit stats debug

Debug process statistics.

```
diagnose sys scanunit stats debug
```

diagnose sys scanunit stats list

List statistics.

```
diagnose sys scanunit stats list
```

diagnose sys scanunit stats manager

scanunit manager statistics.

```
diagnose sys scanunit stats manager
```

diagnose sys scanunit stats worker

scanunit worker statistics.

```
diagnose sys scanunit stats worker
```

diagnose sys scanunit valgrind

Valgrind analysis.

```
diagnose sys scanunit valgrind
```

diagnose sys scanunit valgrind disable

Force daemon to restart.

```
diagnose sys scanunit valgrind disable
```

diagnose sys scanunit valgrind enable

Force daemon to restart.

```
diagnose sys scanunit valgrind enable
```

diagnose sys scanunit valgrind log

Valgrind logs.

```
diagnose sys scanunit valgrind log
```

diagnose sys scanunit valgrind log clear

Clear logs.

```
diagnose sys scanunit valgrind log clear
```


diagnose sys scanunit valgrind log show

Show logs.

```
diagnose sys scanunit valgrind log show
```

diagnose sys scanunit valgrind memcheck

Force daemon to restart.

```
diagnose sys scanunit valgrind memcheck
```

diagnose sys scanunit valgrind memcheck_less

Force daemon to restart.

```
diagnose sys scanunit valgrind memcheck_less
```

diagnose sys scanunit valgrind status

Show valgrind status.

```
diagnose sys scanunit valgrind status
```

diagnose sys scanunit vdom-stats

Current VDOM statistics.

```
diagnose sys scanunit vdom-stats
```

diagnose sys scanunit vdom-stats all

List all VDOM statistics.

```
diagnose sys scanunit vdom-stats all
```

diagnose sys scanunit vdom-stats clear

Clear current VDOM statistics.

```
diagnose sys scanunit vdom-stats clear
```

diagnose sys scanunit vdom-stats clear-all

Clear all VDOM statistics.

```
diagnose sys scanunit vdom-stats clear-all
```

diagnose sys scanunit vdom-stats list

List current VDOM statistics.

```
diagnose sys scanunit vdom-stats list
```

diagnose sys scanunit watchdog-override

Configure scanunit manager watchdog override.

```
diagnose sys scanunit watchdog-override
```

diagnose sys scanunit watchdog-override disable

Disable watchdog override.

```
diagnose sys scanunit watchdog-override disable
```

diagnose sys scanunit watchdog-override enable

Enable watchdog override.

```
diagnose sys scanunit watchdog-override enable
```

diagnose sys scanunit watchdog-override interval

Set watchdog override interval.

```
diagnose sys scanunit watchdog-override interval <time>
```

Parameter	Description	Type	Size
<time>	Override interval (sec) for worker watchdog.	string	

diagnose sys sccp-proxy

SCCP proxy diagnostics.

```
diagnose sys sccp-proxy
```

diagnose sys sccp-proxy debug-console

Debug consoles.

```
diagnose sys sccp-proxy debug-console
```

diagnose sys sccp-proxy phone

SCCP phones.

```
diagnose sys sccp-proxy phone
```

diagnose sys sccp-proxy phone list

List SCCP phones.

```
diagnose sys sccp-proxy phone list
```

diagnose sys sccp-proxy redirect

Redirects

```
diagnose sys sccp-proxy redirect
```

diagnose sys sccp-proxy redirect list

List SIP redirects.

```
diagnose sys sccp-proxy redirect list
```

diagnose sys sccp-proxy restart

Restart SIP and SCCP.

```
diagnose sys sccp-proxy restart
```

diagnose sys sccp-proxy stats

SCCP statistics.

```
diagnose sys sccp-proxy stats
```

diagnose sys sccp-proxy stats clear

Clear SCCP statistics.

```
diagnose sys sccp-proxy stats clear
```

diagnose sys sccp-proxy stats list

List SCCP statistics.

```
diagnose sys sccp-proxy stats list
```

diagnose sys sccp-proxy stats mem

Memory usage.

```
diagnose sys sccp-proxy stats mem
```

diagnose sys sccp-proxy stats mem full

Memory usage details.

```
diagnose sys sccp-proxy stats mem full
```

diagnose sys sccp-proxy stats mem summary

Memory usage summary.

```
diagnose sys sccp-proxy stats mem summary
```

diagnose sys sccp-proxy stats proto

SCCP proxy general protocol statistics summary.

```
diagnose sys sccp-proxy stats proto
```

diagnose sys sccp-proxy valgrind

Valgrind analysis.

```
diagnose sys sccp-proxy valgrind
```

diagnose sys sccp-proxy valgrind disable

Force daemon to restart.

```
diagnose sys sccp-proxy valgrind disable
```

diagnose sys sccp-proxy valgrind enable

Force daemon to restart.

```
diagnose sys sccp-proxy valgrind enable
```

diagnose sys sccp-proxy valgrind log

Valgrind logs.

```
diagnose sys sccp-proxy valgrind log
```

diagnose sys sccp-proxy valgrind log clear

Clear logs.

```
diagnose sys sccp-proxy valgrind log clear
```

diagnose sys sccp-proxy valgrind log show

Show logs.

```
diagnose sys sccp-proxy valgrind log show
```

diagnose sys sccp-proxy valgrind memcheck

Force daemon to restart.

```
diagnose sys sccp-proxy valgrind memcheck
```

diagnose sys sccp-proxy valgrind memcheck_less

Force daemon to restart.

```
diagnose sys sccp-proxy valgrind memcheck_less
```

diagnose sys sccp-proxy valgrind status

Show valgrind status.

```
diagnose sys sccp-proxy valgrind status
```

diagnose sys sdn

SDN Connector diagnostics.

```
diagnose sys sdn
```

diagnose sys sdn cache

Show SDN Connector cache.

```
diagnose sys sdn cache <sdn-data-type> <sdn-connector-name>
```

Parameter	Description	Type	Size
<sdn-data-type>	Specify the data type of the SDN Connector: address/service.	string	
<sdn-connector-name>	Specify the name of the SDN connector.	string	

diagnose sys sdn status

Show SDN Connector status.

```
diagnose sys sdn status <sdn-connector-name> <server-ip-address>
```

Parameter	Description	Type	Size
<sdn-connector-name>	Specify the name of the SDN Connector.	string	
<server-ip-address>	Specify the IP address of the SDN connector.	string	

diagnose sys sdwan

SD-WAN.

```
diagnose sys sdwan
```

diagnose sys sdwan advpn

Show health check info of advpn in SD-WAN.

```
diagnose sys sdwan advpn <num-info>
```

Parameter	Description	Type	Size
<num-info>	num of SDWAN members.	string	

diagnose sys sdwan advpn-session

Show advpn session info.

```
diagnose sys sdwan advpn-session
```

diagnose sys sdwan health-check

Health Check.

```
diagnose sys sdwan health-check
```

diagnose sys sdwan health-check filter

Filter health-check

```
diagnose sys sdwan health-check filter
```

diagnose sys sdwan health-check filter clear

Clear all filters.

```
diagnose sys sdwan health-check filter clear
```

diagnose sys sdwan health-check filter member

Member sequence numbers <seq>.

```
diagnose sys sdwan health-check filter member <member>
```


Parameter	Description	Type	Size
<member>	Member sequence numbers.	string	

diagnose sys sdwan health-check filter name

Health Check names <name>.

```
diagnose sys sdwan health-check filter name <name>
```

Parameter	Description	Type	Size
<name>	Health Check name.	string	

diagnose sys sdwan health-check remote

Remote health check.

```
diagnose sys sdwan health-check remote <name> <seq-num>
```

Parameter	Description	Type	Size
<name>	Show status of the remote health check.	string	
<seq-num>	Sequence number of the member.	string	

diagnose sys sdwan health-check status

Health Check Status.

```
diagnose sys sdwan health-check status <name>
```

Parameter	Description	Type	Size
<name>	Show running status of the health check in SD-WAN.	string	

diagnose sys sdwan internet-service-app-ctrl-3t-set

Set application control Internet Service 3T Info: ctrl-app-id, IP address, protocol & port

```
diagnose sys sdwan internet-service-app-ctrl-3t-set <ctrl-app-id> <ip> <proto> <port>
```

Parameter	Description	Type	Size
<ctrl-app-id>	ctrl app id	string	
<ip>	Service IP address.	string	
<proto>	Service protocol(0-255) for instance: tcp is 6	string	
<port>	Service port(0-65535).	string	

diagnose sys sdwan internet-service-app-ctrl-3t-unset

Unset application control Internet Service 3T Info: ctrl-app-id, IP address, protocol & port

```
diagnose sys sdwan internet-service-app-ctrl-3t-unset <ctrl-app-id> <ip> <proto> <port>
```

Parameter	Description	Type	Size
<ctrl-app-id>	ctrl app id	string	
<ip>	Service IP address.	string	
<proto>	Service protocol(0-255) for instance: tcp is 6	string	
<port>	Service port(0-65535).	string	

diagnose sys sdwan internet-service-app-ctrl-flush

Flush application control Internet Service.

```
diagnose sys sdwan internet-service-app-ctrl-flush
```

diagnose sys sdwan internet-service-app-ctrl-list

Show application control Internet Service ID list.

```
diagnose sys sdwan internet-service-app-ctrl-list
```

diagnose sys sdwan internet-service-app-ctrl-list app-id

Show application control Internet Service ID info of one given application id.

```
diagnose sys sdwan internet-service-app-ctrl-list app-id <app-id>
```

Parameter	Description	Type	Size
<app-id>	application control id.	string	

diagnose sys sdwan internet-service-app-ctrl-list cat-id

Show application control Internet Service ID info of one given application category id.

```
diagnose sys sdwan internet-service-app-ctrl-list cat-id <cat-id>
```

Parameter	Description	Type	Size
<cat-id>	application category id.	string	

diagnose sys sdwan internet-service-app-ctrl6-3t-set

Set application control6 Internet Service 3T Info: ctrl-app-id, IP address, protocol & port

```
diagnose sys sdwan internet-service-app-ctrl6-3t-set <ctrl-app-id> <ip> <proto> <port>
```

Parameter	Description	Type	Size
<ctrl-app-id>	ctrl app id	string	
<ip>	Service IP address(Ipv6).	string	
<proto>	Service protocol(0-255) for instance: tcp is 6	string	
<port>	Service port(0-65535).	string	

diagnose sys sdwan internet-service-app-ctrl6-3t-unset

Unset application control6 Internet Service 3T Info: ctrl-app-id, IP address, protocol & port

```
diagnose sys sdwan internet-service-app-ctrl6-3t-unset <ctrl-app-id> <ip> <proto> <port>
```

Parameter	Description	Type	Size
<ctrl-app-id>	ctrl app id	string	
<ip>	Service IP address(Ipv6).	string	
<proto>	Service protocol(0-255) for instance: tcp is 6	string	
<port>	Service port(0-65535).	string	

diagnose sys sdwan internet-service-app-ctrl6-flush

Flush application control Internet Service6.

```
diagnose sys sdwan internet-service-app-ctrl6-flush
```

diagnose sys sdwan internet-service-app-ctrl6-list

Show application control Internet Service6 ID list.

```
diagnose sys sdwan internet-service-app-ctrl6-list
```

diagnose sys sdwan internet-service-app-ctrl6-list app-id

Show application control Internet Service6 ID info of one given application id.

```
diagnose sys sdwan internet-service-app-ctrl6-list app-id <app-id>
```

Parameter	Description	Type	Size
<app-id>	application control id.	string	

diagnose sys sdwan internet-service-app-ctrl6-list cat-id

Show application control Internet Service6 ID info of one given application category id.

```
diagnose sys sdwan internet-service-app-ctrl6-list cat-id <cat-id>
```

Parameter	Description	Type	Size
<cat-id>	application category id.	string	

diagnose sys sdwan intf-sla-log

Show details of interface quality information.

```
diagnose sys sdwan intf-sla-log <name>
```

Parameter	Description	Type	Size
<name>	Interface name.	string	

diagnose sys sdwan log

Log.

```
diagnose sys sdwan log <service-id>
```

Parameter	Description	Type	Size
<service-id>	Show details of traffic log on service in SD-WAN.	string	

diagnose sys sdwan member

Member.

```
diagnose sys sdwan member <seq-num>
```

Parameter	Description	Type	Size
<seq-num>	Show details of member in SD-WAN.	string	

diagnose sys sdwan neighbor

Neighbor.

```
diagnose sys sdwan neighbor <name>
```

Parameter	Description	Type	Size
<name>	Show running status of the neighbor in SD-WAN.	string	

diagnose sys sdwan reset

Reset SD-WAN.

```
diagnose sys sdwan reset
```

diagnose sys sdwan route

Dump SD-WAN routes.

```
diagnose sys sdwan route <seq-num>
```

Parameter	Description	Type	Size
<seq-num>	Show details of SD-WAN routes.	string	

diagnose sys sdwan route6

Dump IPv6 SD-WAN routes.

```
diagnose sys sdwan route6 <seq-num>
```

Parameter	Description	Type	Size
<seq-num>	Show details of IPv6 SD-WAN routes.	string	

diagnose sys sdwan service4

IPv4 Service.

```
diagnose sys sdwan service4 <id>
```

Parameter	Description	Type	Size
<id>	Show details of IPv4 service in SD-WAN.	string	

diagnose sys sdwan service6

IPv6 Service.

```
diagnose sys sdwan service6 <id>
```

Parameter	Description	Type	Size
<id>	Show details of IPv6 service in SD-WAN.	string	

diagnose sys sdwan sla-log

Show details of health-check quality information in last 10 minutes

```
diagnose sys sdwan sla-log <name> <seq-num> <childname>
```

Parameter	Description	Type	Size
<name>	Health check name.	string	
<seq-num>	Sequence number of the member.	string	
<childname>	Child interface name.	string	

diagnose sys sdwan zone

Dump sdwan zone info in kernel.

```
diagnose sys sdwan zone
```

diagnose sys server-probe

Server probe.

```
diagnose sys server-probe
```

diagnose sys server-probe response

Probe response.

```
diagnose sys server-probe response
```

diagnose sys service-communication

Show historical statistics for communication with FortiGuard services.

```
diagnose sys service-communication
```

diagnose sys session

IPv4 session.

```
diagnose sys session
```

diagnose sys session clear

Clear the sessions defined by filter.

```
diagnose sys session clear
```

diagnose sys session exp-stat

Expectation session statistics.

```
diagnose sys session exp-stat
```

diagnose sys session filter

List session with filters.

```
diagnose sys session filter
```

diagnose sys session filter clear

Clear session filter.

```
diagnose sys session filter clear
```

diagnose sys session filter clear dintf

Clear destination interface filter.

```
diagnose sys session filter clear dintf
```

diagnose sys session filter clear dport

Clear destination port filter.

```
diagnose sys session filter clear dport
```


diagnose sys session filter clear dst

Clear destination IP filter.

```
diagnose sys session filter clear dst
```

diagnose sys session filter clear duration

Clear duration filter.

```
diagnose sys session filter clear duration
```

diagnose sys session filter clear expire

Clear expire filter.

```
diagnose sys session filter clear expire
```

diagnose sys session filter clear nport

clear NAT'd source port filter

```
diagnose sys session filter clear nport
```

diagnose sys session filter clear nsrc

clear NAT'd source IP filter

```
diagnose sys session filter clear nsrc
```

diagnose sys session filter clear policy

Clear policy ID filter.

```
diagnose sys session filter clear policy
```

diagnose sys session filter clear proto

Clear protocol filter.

```
diagnose sys session filter clear proto
```

diagnose sys session filter clear proto-state

Clear protocol state filter.

```
diagnose sys session filter clear proto-state
```

diagnose sys session filter clear session-state1

Clear session-state1 filter.

```
diagnose sys session filter clear session-state1
```

diagnose sys session filter clear session-state2

Clear session-state2 filter.

```
diagnose sys session filter clear session-state2
```

diagnose sys session filter clear sintf

Clear source interface filter.

```
diagnose sys session filter clear sintf
```

diagnose sys session filter clear sport

Clear source port filter.

```
diagnose sys session filter clear sport
```

diagnose sys session filter clear src

Clear source IP filter.

```
diagnose sys session filter clear src
```

diagnose sys session filter clear vd

Clear virtual domain filter.

```
diagnose sys session filter clear vd
```

diagnose sys session filter dintf

Destination interface.

```
diagnose sys session filter dintf <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	Interface name.	string	

diagnose sys session filter dport

Destination port.

```
diagnose sys session filter dport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys session filter dst

Destination IP address.

```
diagnose sys session filter dst <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP (from).	string	
<xxx.xxx.xxx.xxx>	Destination IP (to).	string	

diagnose sys session filter duration

duration

```
diagnose sys session filter duration <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Duration (from).	string	
<xxx>	Duration (to).	string	

diagnose sys session filter expire

expire

```
diagnose sys session filter expire <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Expire (from).	string	
<xxx>	Expire (to).	string	

diagnose sys session filter ext-dst

Add a destination address to the extended match list.

```
diagnose sys session filter ext-dst <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP.	string	

diagnose sys session filter ext-dst-negate

Add a destination address to the negated extended match list.

```
diagnose sys session filter ext-dst-negate <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP.	string	

diagnose sys session filter ext-src

Add a source address to the extended match list.

```
diagnose sys session filter ext-src <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP.	string	

diagnose sys session filter ext-src-negate

Add a source address to the negated extended match list.

```
diagnose sys session filter ext-src-negate <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP.	string	

diagnose sys session filter negate

Inverse filter.

```
diagnose sys session filter negate
```

diagnose sys session filter negate dintf

Inverse destination interface.

```
diagnose sys session filter negate dintf
```

diagnose sys session filter negate dport

Inverse destination port.

```
diagnose sys session filter negate dport
```

diagnose sys session filter negate dst

Inverse destination IP.

```
diagnose sys session filter negate dst
```

diagnose sys session filter negate duration

Inverse duration.

```
diagnose sys session filter negate duration
```

diagnose sys session filter negate expire

Inverse expire.

```
diagnose sys session filter negate expire
```

diagnose sys session filter negate nport

inverse NAT'd source port

```
diagnose sys session filter negate nport
```

diagnose sys session filter negate nsrc

inverse NAT'd source IP

```
diagnose sys session filter negate nsrc
```

diagnose sys session filter negate policy

Inverse policy ID.

```
diagnose sys session filter negate policy
```

diagnose sys session filter negate proto

Inverse protocol.

```
diagnose sys session filter negate proto
```

diagnose sys session filter negate proto-state

Inverse protocol state.

```
diagnose sys session filter negate proto-state
```

diagnose sys session filter negate session-state1

Inverse session-state1.

```
diagnose sys session filter negate session-state1
```

diagnose sys session filter negate session-state2

Inverse session-state2.

```
diagnose sys session filter negate session-state2
```

diagnose sys session filter negate intf

Inverse source interface.

```
diagnose sys session filter negate intf
```

diagnose sys session filter negate sport

Inverse source port.

```
diagnose sys session filter negate sport
```

diagnose sys session filter negate src

Inverse source IP.

```
diagnose sys session filter negate src
```

diagnose sys session filter negate vd

Inverse virtual domain.

```
diagnose sys session filter negate vd
```

diagnose sys session filter nport

NAT'd source port

```
diagnose sys session filter nport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys session filter nsrc

NAT'd source ip address

```
diagnose sys session filter nsrc <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	NAT'd source ip (from)	string	
<xxx.xxx.xxx.xxx>	NAT'd source ip (to)	string	

diagnose sys session filter policy

Policy ID.

```
diagnose sys session filter policy <xxx> <xxx>
```


Parameter	Description	Type	Size
<xxx>	Policy ID (from).	string	
<xxx>	Policy ID (to).	string	

diagnose sys session filter proto

Protocol number.

```
diagnose sys session filter proto <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255> (from).	string	
<xx>	<0-255> (to).	string	

diagnose sys session filter proto-state

Protocol state.

```
diagnose sys session filter proto-state <x> <x>
```

Parameter	Description	Type	Size
<x>	<0-9> (from). 0: ANY 1: TCP_S_ESTABLISHED, SCTP_S_ESTABLISHED 2: TCP_S_SYN_SENT, SCTP_S_CLOSED 3: TCP_S_SYN_RECV, SCTP_S_COOKIE_WAIT 4: TCP_S_FIN_WAIT, SCTP_S_COOKIE_ECHOED 5: TCP_S_TIME_WAIT, SCTP_S_SHUTDOWN_SENT 6: TCP_S_CLOSE, SCTP_S_SHUTDOWN_RECV 7: TCP_S_CLOSE_WAIT, SCTP_S_SHUTDOWN_ACK_SENT 8: TCP_S_LAST_ACK 9: TCP_S_LISTEN	string	
<x>	<0-9> (to). 0: ANY 1: TCP_S_ESTABLISHED, SCTP_S_ESTABLISHED 2: TCP_S_SYN_SENT, SCTP_S_CLOSED 3: TCP_S_SYN_RECV, SCTP_S_COOKIE_WAIT 4: TCP_S_FIN_WAIT, SCTP_S_COOKIE_ECHOED 5: TCP_S_TIME_WAIT, SCTP_S_SHUTDOWN_SENT 6: TCP_S_CLOSE, SCTP_S_SHUTDOWN_RECV 7: TCP_S_CLOSE_WAIT, SCTP_S_SHUTDOWN_ACK_SENT 8: TCP_S_LAST_ACK 9: TCP_S_LISTEN	string	

diagnose sys session filter session-state1

Session state1.

```
diagnose sys session filter session-state1 <x> <x>
```

Parameter	Description	Type	Size
<x>	<0-FFFFFFFF>, state bits.	string	
<x>	<0-FFFFFFFF>, state bit mask.	string	

diagnose sys session filter session-state2

Session state2.

```
diagnose sys session filter session-state2 <x> <x>
```

Parameter	Description	Type	Size
<x>	<0-FFFFFFFF>, state bits.	string	
<x>	<0-FFFFFFFF>, state bit mask.	string	

diagnose sys session filter sintf

Source interface.

```
diagnose sys session filter sintf <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	Interface name.	string	

diagnose sys session filter sport

Source port.

```
diagnose sys session filter sport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys session filter src

Source IP address.

```
diagnose sys session filter src <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (from).	string	
<xxx.xxx.xxx.xxx>	Source IP (to).	string	

diagnose sys session filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys session filter vd <xxx>
```

Parameter	Description	Type	Size
<xxx>	Index of virtual domain. -1 matches all.	string	

diagnose sys session filter vd-name

Name of virtual domain. -1 or "any" matches all.

```
diagnose sys session filter vd-name <...>
```

Parameter	Description	Type	Size
<...>	Name of virtual domain. -1 or "any" matches all.	string	

diagnose sys session full-stat

Fully stat session.

```
diagnose sys session full-stat
```

diagnose sys session help

Session help.

```
diagnose sys session help
```

diagnose sys session help add

Add session help.

```
diagnose sys session help add <name> <protocol> <port>
```

Parameter	Description	Type	Size
<name>	Help name.	string	
<protocol>	Protocol number.	string	
<port>	Help port.	string	

diagnose sys session help delete

Delete session help.

```
diagnose sys session help delete <protocol> <port>
```

Parameter	Description	Type	Size
<protocol>	Protocol number.	string	
<port>	Help port.	string	

diagnose sys session help list

List session help.

```
diagnose sys session help list
```

diagnose sys session list

List session.

```
diagnose sys session list
```

diagnose sys session list expectation

List expectation session.

```
diagnose sys session list expectation
```

diagnose sys session stat

Stat session.

```
diagnose sys session stat
```

diagnose sys session sync

List session sync.

```
diagnose sys session sync
```

diagnose sys session sync reset

Reset session sync.

```
diagnose sys session sync reset
```

diagnose sys session ttl

TTL session.

```
diagnose sys session ttl
```

diagnose sys session6

IPv6 session.

```
diagnose sys session6
```

diagnose sys session6 clear

Clear IPv6 sessions defined by filter.

```
diagnose sys session6 clear
```

diagnose sys session6 exp-stat

Expectation session statistics.

```
diagnose sys session6 exp-stat
```

diagnose sys session6 filter

List IPv6 session with filters.

```
diagnose sys session6 filter
```

diagnose sys session6 filter clear

Clear IPv6 session filter.

```
diagnose sys session6 filter clear
```

diagnose sys session6 filter clear dintf

Clear destination interface filter.

```
diagnose sys session6 filter clear dintf
```

diagnose sys session6 filter clear dport

Clear destination port filter.

```
diagnose sys session6 filter clear dport
```

diagnose sys session6 filter clear dst

Clear destination IP filter.

```
diagnose sys session6 filter clear dst
```

diagnose sys session6 filter clear duration

Clear duration filter.

```
diagnose sys session6 filter clear duration
```

diagnose sys session6 filter clear expire

Clear expire filter.

```
diagnose sys session6 filter clear expire
```

diagnose sys session6 filter clear nport

Clear NAT'd source port filter.

```
diagnose sys session6 filter clear nport
```

diagnose sys session6 filter clear nsrc

Clear NAT'd source IP filter.

```
diagnose sys session6 filter clear nsrc
```

diagnose sys session6 filter clear policy

Clear policy ID filter.

```
diagnose sys session6 filter clear policy
```

diagnose sys session6 filter clear proto

Clear protocol filter.

```
diagnose sys session6 filter clear proto
```

diagnose sys session6 filter clear proto-state

Clear protocol state filter.

```
diagnose sys session6 filter clear proto-state
```

diagnose sys session6 filter clear session-state1

Clear session-state1 filter.

```
diagnose sys session6 filter clear session-state1
```

diagnose sys session6 filter clear session-state2

Clear session-state2 filter.

```
diagnose sys session6 filter clear session-state2
```

diagnose sys session6 filter clear sintf

Clear source interface filter.

```
diagnose sys session6 filter clear sintf
```

diagnose sys session6 filter clear sport

Clear source port filter.

```
diagnose sys session6 filter clear sport
```

diagnose sys session6 filter clear src

Clear source IP filter.

```
diagnose sys session6 filter clear src
```


diagnose sys session6 filter clear vd

Clear virtual domain filter.

```
diagnose sys session6 filter clear vd
```

diagnose sys session6 filter dintf

Destination interface.

```
diagnose sys session6 filter dintf <xxxxx>
```

Parameter	Description	Type	Size
<xxxxx>	Interface name.	string	

diagnose sys session6 filter dport

Destination port.

```
diagnose sys session6 filter dport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys session6 filter dst

Destination IP address.

```
diagnose sys session6 filter dst <xxx:xxx::xxx:xxx> <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Destination IP (from).	string	
<xxx:xxx::xxx:xxx>	Destination IP (to).	string	

diagnose sys session6 filter duration

duration

```
diagnose sys session6 filter duration <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Duration (from).	string	
<xxx>	Duration (to).	string	

diagnose sys session6 filter expire

expire

```
diagnose sys session6 filter expire <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Expire (from).	string	
<xxx>	Expire (to).	string	

diagnose sys session6 filter ext-dst

Add a destination address to the extended match list.

```
diagnose sys session6 filter ext-dst <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Destination IP.	string	

diagnose sys session6 filter ext-dst-negate

Add a destination address to the negated extended match list.

```
diagnose sys session6 filter ext-dst-negate <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Destination IP.	string	

diagnose sys session6 filter ext-src

Add a source address to the extended match list.

```
diagnose sys session6 filter ext-src <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Source IP.	string	

diagnose sys session6 filter ext-src-negate

Add a source address to the negated extended match list.

```
diagnose sys session6 filter ext-src-negate <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Source IP.	string	

diagnose sys session6 filter negate

Inverse filter.

```
diagnose sys session6 filter negate
```

diagnose sys session6 filter negate dintf

Inverse destination interface.

```
diagnose sys session6 filter negate dintf
```

diagnose sys session6 filter negate dport

Inverse destination port.

```
diagnose sys session6 filter negate dport
```

diagnose sys session6 filter negate dst

Inverse destination IP.

```
diagnose sys session6 filter negate dst
```

diagnose sys session6 filter negate duration

Inverse duration.

```
diagnose sys session6 filter negate duration
```

diagnose sys session6 filter negate expire

Inverse expire.

```
diagnose sys session6 filter negate expire
```

diagnose sys session6 filter negate nport

Inverse NAT'd source port.

```
diagnose sys session6 filter negate nport
```

diagnose sys session6 filter negate nsrc

Inverse NAT'd source IP.

```
diagnose sys session6 filter negate nsrc
```

diagnose sys session6 filter negate policy

Inverse policy ID.

```
diagnose sys session6 filter negate policy
```

diagnose sys session6 filter negate proto

Inverse protocol.

```
diagnose sys session6 filter negate proto
```

diagnose sys session6 filter negate proto-state

Inverse protocol state.

```
diagnose sys session6 filter negate proto-state
```

diagnose sys session6 filter negate session-state1

Inverse session-state1.

```
diagnose sys session6 filter negate session-state1
```

diagnose sys session6 filter negate session-state2

Inverse session-state2.

```
diagnose sys session6 filter negate session-state2
```

diagnose sys session6 filter negate sintf

Inverse source interface.

```
diagnose sys session6 filter negate sintf
```

diagnose sys session6 filter negate sport

Inverse source port.

```
diagnose sys session6 filter negate sport
```

diagnose sys session6 filter negate src

Inverse source IP.

```
diagnose sys session6 filter negate src
```

diagnose sys session6 filter negate vd

Inverse virtual domain.

```
diagnose sys session6 filter negate vd
```

diagnose sys session6 filter nport

NAT'd source port.

```
diagnose sys session6 filter nport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys session6 filter nsrc

NAT'd source IP address.

```
diagnose sys session6 filter nsrc <xxx:xxx::xxx:xxx> <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	NAT'd source IP (from).	string	
<xxx:xxx::xxx:xxx>	NAT'd Source IP (to).	string	

diagnose sys session6 filter policy

Policy ID.

```
diagnose sys session6 filter policy <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Policy ID (from).	string	
<xxx>	Policy ID (to).	string	

diagnose sys session6 filter proto

Protocol number.

```
diagnose sys session6 filter proto <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255> (from).	string	
<xx>	<0-255> (to).	string	

diagnose sys session6 filter proto-state

Protocol state.

```
diagnose sys session6 filter proto-state <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255> (from).	string	
<xx>	<0-255> (to).	string	

diagnose sys session6 filter session-state1

Session state1.

```
diagnose sys session6 filter session-state1 <x> <x>
```

Parameter	Description	Type	Size
<x>	<0-FFFFFFFF>, state bits.	string	
<x>	<0-FFFFFFFF>, state bit mask.	string	

diagnose sys session6 filter session-state2

Session state2.

```
diagnose sys session6 filter session-state2 <x> <x>
```

Parameter	Description	Type	Size
<x>	<0-FFFFFFFF>, state bits.	string	
<x>	<0-FFFFFFFF>, state bit mask.	string	

diagnose sys session6 filter sintf

Source interface.

```
diagnose sys session6 filter sintf <xxxxx>
```

Parameter	Description	Type	Size
<xxxxx>	Interface name.	string	

diagnose sys session6 filter sport

Source port.

```
diagnose sys session6 filter sport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

diagnose sys session6 filter src

Source IP address.

```
diagnose sys session6 filter src <xxx:xxx::xxx:xxx> <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Source IP (from).	string	
<xxx:xxx::xxx:xxx>	Source IP (to).	string	

diagnose sys session6 filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys session6 filter vd <xxx>
```


Parameter	Description	Type	Size
<xxx>	Index of virtual domain. -1 matches all.	string	

diagnose sys session6 filter vd-name

name of virtual domain. -1 or "any" matches all.

```
diagnose sys session6 filter vd-name <...>
```

Parameter	Description	Type	Size
<...>	Name of virtual domain. -1 or "any" matches all.	string	

diagnose sys session6 full-stat

Fully stat session.

```
diagnose sys session6 full-stat
```

diagnose sys session6 help

IPv6 session help.

```
diagnose sys session6 help
```

diagnose sys session6 help add

Add session help.

```
diagnose sys session6 help add <name> <protocol> <port>
```

Parameter	Description	Type	Size
<name>	Help name.	string	
<protocol>	Protocol number.	string	
<port>	Help port.	string	

diagnose sys session6 help delete

Delete session help.

```
diagnose sys session6 help delete <protocol> <port>
```

Parameter	Description	Type	Size
<protocol>	Protocol number.	string	
<port>	Help port.	string	

diagnose sys session6 help list

List IPv6 session help.

```
diagnose sys session6 help list
```

diagnose sys session6 list

List IPv6 session.

```
diagnose sys session6 list
```

diagnose sys session6 list expectation

List IPv6 expectation session.

```
diagnose sys session6 list expectation
```

diagnose sys session6 stat

Stat session.

```
diagnose sys session6 stat
```

diagnose sys session6 sync

List session6 sync.

```
diagnose sys session6 sync
```

diagnose sys session6 sync reset

Reset session6 sync.

```
diagnose sys session6 sync reset
```

diagnose sys shmfile

shmfile related information.

```
diagnose sys shmfile
```

diagnose sys shmfile dump

dump.

```
diagnose sys shmfile dump
```

diagnose sys shmfile dump oid-app

oid-app information.

```
diagnose sys shmfile dump oid-app <path.name>
```

Parameter	Description	Type	Size
<path.name>	object's path.name.	string	

diagnose sys shmfile dump oid-slab

oid-slab information.

```
diagnose sys shmfile dump oid-slab <path.object>
```

Parameter	Description	Type	Size
<path.object>	vdom root object's information.	string	

diagnose sys shmfile dump slab-file

slab file information.

```
diagnose sys shmfile dump slab-file [file]
```

Parameter	Description	Type	Size
[file]	file name.	string	

diagnose sys shmfile dump table-count

table count information.

```
diagnose sys shmfile dump table-count
```

diagnose sys shmfile dump table-count total

total table count information.

```
diagnose sys shmfile dump table-count total <path.name>
```

Parameter	Description	Type	Size
<path.name>	object's path.name (e.g. system.interface).	string	

diagnose sys shmfile dump table-count vdom

vdom table count information.

```
diagnose sys shmfile dump table-count vdom <vdom-name> <path.name>
```

Parameter	Description	Type	Size
<vdom-name>	vdom name.	string	
<path.name>	object's path.name (e.g. system.interface).	string	

diagnose sys shmfile dump vdom

vdom information.

```
diagnose sys shmfile dump vdom <vdom-name>
```

Parameter	Description	Type	Size
<vdom-name>	vdom name.	string	

diagnose sys sip

SIP diagnostics.

```
diagnose sys sip
```

diagnose sys sip debug-mask

Mask for SIP kernel trace.

```
diagnose sys sip debug-mask <mask>
```

Parameter	Description	Type	Size
<mask>	For example, 0, 1, 2, 3 ...	string	

diagnose sys sip dialog

SIP dialog.

```
diagnose sys sip dialog
```

diagnose sys sip dialog clear

Clear SIP dialogs.

```
diagnose sys sip dialog clear
```

diagnose sys sip dialog list

List SIP dialogs.

```
diagnose sys sip dialog list
```

diagnose sys sip mapping

SIP mapping.

```
diagnose sys sip mapping
```

diagnose sys sip mapping list

List SIP mappings.

```
diagnose sys sip mapping list
```

diagnose sys sip status

Display SIP status.

```
diagnose sys sip status
```

diagnose sys sip-proxy

SIP proxy diagnostics.

```
diagnose sys sip-proxy
```

diagnose sys sip-proxy alg

SIP to ALG passing.

```
diagnose sys sip-proxy alg
```

diagnose sys sip-proxy alg bypass

Pass SIP to ALG but pass it directly through without parsing.

```
diagnose sys sip-proxy alg bypass
```

diagnose sys sip-proxy alg parse-only

Pass SIP to ALG and parse but do not modify.

```
diagnose sys sip-proxy alg parse-only
```

diagnose sys sip-proxy calls

SIP calls.

```
diagnose sys sip-proxy calls
```

diagnose sys sip-proxy calls clear

Clear all active SIP calls.

```
diagnose sys sip-proxy calls clear
```

diagnose sys sip-proxy calls idle

List idle SIP calls.

```
diagnose sys sip-proxy calls idle
```

diagnose sys sip-proxy calls invite

List SIP invite transactions.

```
diagnose sys sip-proxy calls invite
```

diagnose sys sip-proxy calls list

List active SIP calls.

```
diagnose sys sip-proxy calls list
```

diagnose sys sip-proxy config

Configuration details.

```
diagnose sys sip-proxy config
```

diagnose sys sip-proxy config list

Display SIP per-policy configurations.

```
diagnose sys sip-proxy config list
```

diagnose sys sip-proxy config profiles

Display SIP VoIP profiles.

```
diagnose sys sip-proxy config profiles
```

diagnose sys sip-proxy debug-console

Debug consoles.

```
diagnose sys sip-proxy debug-console
```

diagnose sys sip-proxy filter

Filter for listing meters and calls.

```
diagnose sys sip-proxy filter
```

diagnose sys sip-proxy filter clear

Erase the current filter.

```
diagnose sys sip-proxy filter clear
```


diagnose sys sip-proxy filter dst-addr4

Destination address range to filter by.

```
diagnose sys sip-proxy filter dst-addr4 <ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Destination IPv4 address (from).	string	
<ipv4-address>	Destination IPv4 address (to).	string	

diagnose sys sip-proxy filter dst-addr6

IPv6 destination address range to filter by.

```
diagnose sys sip-proxy filter dst-addr6 <ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Destination IPv6 address (from).	string	
<ipv6-address>	Destination IPv6 address (to).	string	

diagnose sys sip-proxy filter dst-port

Destination port to filter by.

```
diagnose sys sip-proxy filter dst-port <port>
```

Parameter	Description	Type	Size
<port>	Source port.	string	

diagnose sys sip-proxy filter list

Display the current filter.

```
diagnose sys sip-proxy filter list
```

diagnose sys sip-proxy filter negate

Negate the specified filter parameter.

```
diagnose sys sip-proxy filter negate
```

diagnose sys sip-proxy filter negate dst-addr4

Negate the dst-addr4 filter.

```
diagnose sys sip-proxy filter negate dst-addr4
```

diagnose sys sip-proxy filter negate dst-addr6

Negate the dst-addr6 filter.

```
diagnose sys sip-proxy filter negate dst-addr6
```

diagnose sys sip-proxy filter negate dst-port

Negate the dst-port filter.

```
diagnose sys sip-proxy filter negate dst-port
```

diagnose sys sip-proxy filter negate policy

Negate the policy filter.

```
diagnose sys sip-proxy filter negate policy
```

diagnose sys sip-proxy filter negate policy-type

Negate the policy-type filter.

```
diagnose sys sip-proxy filter negate policy-type
```

diagnose sys sip-proxy filter negate src-addr4

Negate the src-addr4 filter.

```
diagnose sys sip-proxy filter negate src-addr4
```

diagnose sys sip-proxy filter negate src-addr6

Negate the src-addr6 filter.

```
diagnose sys sip-proxy filter negate src-addr6
```

diagnose sys sip-proxy filter negate src-port

Negate the src-port filter.

```
diagnose sys sip-proxy filter negate src-port
```

diagnose sys sip-proxy filter negate vd

Negate the virtual domain filter.

```
diagnose sys sip-proxy filter negate vd
```

diagnose sys sip-proxy filter negate voip-profile

Negate the VoIP-profile filter.

```
diagnose sys sip-proxy filter negate voip-profile
```

diagnose sys sip-proxy filter policy

Policy to filter by.

```
diagnose sys sip-proxy filter policy <policy>
```

Parameter	Description	Type	Size
<policy>	policy	string	

diagnose sys sip-proxy filter policy-type

Policy-type to filter by.

```
diagnose sys sip-proxy filter policy-type
```

diagnose sys sip-proxy filter policy-type ipv4

Filter IPv4 policies.

```
diagnose sys sip-proxy filter policy-type ipv4
```

diagnose sys sip-proxy filter policy-type ipv6

Filter IPv6 policies.

```
diagnose sys sip-proxy filter policy-type ipv6
```

diagnose sys sip-proxy filter src-addr4

Source address range to filter by.

```
diagnose sys sip-proxy filter src-addr4 <ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Source IPv4 address (from).	string	
<ipv4-address>	Source IPv4 address (to).	string	

diagnose sys sip-proxy filter src-addr6

IPv6 source address range to filter by.

```
diagnose sys sip-proxy filter src-addr6 <ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Source IPv6 address (from).	string	
<ipv6-address>	Source IPv6 address (to).	string	

diagnose sys sip-proxy filter src-port

Source port to filter by.

```
diagnose sys sip-proxy filter src-port <port>
```

Parameter	Description	Type	Size
<port>	Source port.	string	

diagnose sys sip-proxy filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys sip-proxy filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose sys sip-proxy filter voip-profile

VoIP profile to filter by.

```
diagnose sys sip-proxy filter voip-profile <voip-profile>
```

Parameter	Description	Type	Size
<voip-profile>	voip-profile	string	

diagnose sys sip-proxy log-filter

SIP ALG debug log filter.

```
diagnose sys sip-proxy log-filter
```

diagnose sys sip-proxy log-filter clear

Clear the current filter.

```
diagnose sys sip-proxy log-filter clear
```

diagnose sys sip-proxy log-filter dst-addr4

IPv4 destination address range to filter by.

```
diagnose sys sip-proxy log-filter dst-addr4 <ip-address> <ip-address>
```

Parameter	Description	Type	Size
<ip-address>	Destination IPv4 address (from).	string	
<ip-address>	Destination IPv4 address (to).	string	

diagnose sys sip-proxy log-filter dst-addr6

IPv6 destination address range to filter by.

```
diagnose sys sip-proxy log-filter dst-addr6 <ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Destination IPv6 address (from).	string	
<ipv6-address>	Destination IPv6 address (to).	string	

diagnose sys sip-proxy log-filter dst-port

Destination port to filter by.

```
diagnose sys sip-proxy log-filter dst-port <port>
```

Parameter	Description	Type	Size
<port>	Source port.	string	

diagnose sys sip-proxy log-filter list

Display the current filter.

```
diagnose sys sip-proxy log-filter list
```

diagnose sys sip-proxy log-filter negate

Negate the specified filter parameter.

```
diagnose sys sip-proxy log-filter negate
```

diagnose sys sip-proxy log-filter negate dst-addr4

Negate the dst-addr4 filter.

```
diagnose sys sip-proxy log-filter negate dst-addr4
```

diagnose sys sip-proxy log-filter negate dst-addr6

Negate the dst-addr6 filter.

```
diagnose sys sip-proxy log-filter negate dst-addr6
```

diagnose sys sip-proxy log-filter negate dst-port

Negate the dst-port filter.

```
diagnose sys sip-proxy log-filter negate dst-port
```

diagnose sys sip-proxy log-filter negate policy

Negate the policy filter.

```
diagnose sys sip-proxy log-filter negate policy
```

diagnose sys sip-proxy log-filter negate policy-type

Negate the policy-type filter.

```
diagnose sys sip-proxy log-filter negate policy-type
```

diagnose sys sip-proxy log-filter negate src-addr4

Negate the src-addr4 filter.

```
diagnose sys sip-proxy log-filter negate src-addr4
```

diagnose sys sip-proxy log-filter negate src-addr6

Negate the src-addr6 filter.

```
diagnose sys sip-proxy log-filter negate src-addr6
```

diagnose sys sip-proxy log-filter negate src-port

Negate the src-port filter.

```
diagnose sys sip-proxy log-filter negate src-port
```

diagnose sys sip-proxy log-filter negate vd

Negate the virtual domain filter.

```
diagnose sys sip-proxy log-filter negate vd
```

diagnose sys sip-proxy log-filter negate voip-profile

Negate the VoIP-profile filter.

```
diagnose sys sip-proxy log-filter negate voip-profile
```


diagnose sys sip-proxy log-filter policy

Policy to filter by.

```
diagnose sys sip-proxy log-filter policy <policy>
```

Parameter	Description	Type	Size
<policy>	policy	string	

diagnose sys sip-proxy log-filter policy-type

Policy-type to filter by.

```
diagnose sys sip-proxy log-filter policy-type
```

diagnose sys sip-proxy log-filter policy-type ipv4

Filter IPv4 policies.

```
diagnose sys sip-proxy log-filter policy-type ipv4
```

diagnose sys sip-proxy log-filter policy-type ipv6

Filter IPv6 policies.

```
diagnose sys sip-proxy log-filter policy-type ipv6
```

diagnose sys sip-proxy log-filter src-addr4

IPv4 source address range to filter by.

```
diagnose sys sip-proxy log-filter src-addr4 <ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Source IPv4 address (from).	string	
<ipv4-address>	Source IPv4 address (to).	string	

diagnose sys sip-proxy log-filter src-addr6

IPv6 source address range to filter by.

```
diagnose sys sip-proxy log-filter src-addr6 <ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Source IPv6 address (from).	string	
<ipv6-address>	Source IPv6 address (to).	string	

diagnose sys sip-proxy log-filter src-port

Source port to filter by.

```
diagnose sys sip-proxy log-filter src-port <port>
```

Parameter	Description	Type	Size
<port>	Source port.	string	

diagnose sys sip-proxy log-filter vd

Index of virtual domain. -1 matches all.

```
diagnose sys sip-proxy log-filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose sys sip-proxy log-filter voip-profile

VoIP profile to filter by.

```
diagnose sys sip-proxy log-filter voip-profile <voip-profile>
```

Parameter	Description	Type	Size
<voip-profile>	voip-profile	string	

diagnose sys sip-proxy meters

Diagnostics for SIP rate limiting meters.

```
diagnose sys sip-proxy meters
```

diagnose sys sip-proxy meters list

List active SIP rate limiting meters.

```
diagnose sys sip-proxy meters list
```

diagnose sys sip-proxy redirect

Redirects

```
diagnose sys sip-proxy redirect
```

diagnose sys sip-proxy redirect list

List SIP redirects.

```
diagnose sys sip-proxy redirect list
```

diagnose sys sip-proxy restart

Restart SIP and SCCP.

```
diagnose sys sip-proxy restart
```

diagnose sys sip-proxy scheduler-times

Scheduler times.

```
diagnose sys sip-proxy scheduler-times
```

diagnose sys sip-proxy scheduler-times display

Display scheduler times.

```
diagnose sys sip-proxy scheduler-times display
```

diagnose sys sip-proxy scheduler-times start

Start measuring scheduler times.

```
diagnose sys sip-proxy scheduler-times start
```

diagnose sys sip-proxy scheduler-times stop

Stop measuring scheduler times.

```
diagnose sys sip-proxy scheduler-times stop
```

diagnose sys sip-proxy session

SIP sessions.

```
diagnose sys sip-proxy session
```

diagnose sys sip-proxy session list

List SIP sessions.

```
diagnose sys sip-proxy session list
```

diagnose sys sip-proxy ssl

SSL hardware support.

```
diagnose sys sip-proxy ssl
```

diagnose sys sip-proxy ssl hardware

Enable SSL hardware support (default) (will restart voip).

```
diagnose sys sip-proxy ssl hardware
```

diagnose sys sip-proxy ssl software

Disable SSL hardware support (will restart voip).

```
diagnose sys sip-proxy ssl software
```

diagnose sys sip-proxy stats

SIP proxy statistics.

```
diagnose sys sip-proxy stats
```

diagnose sys sip-proxy stats call

SIP proxy call statistics summary.

```
diagnose sys sip-proxy stats call
```

diagnose sys sip-proxy stats clear

Clear SIP proxy activity statistics.

```
diagnose sys sip-proxy stats clear
```

diagnose sys sip-proxy stats ha

SIP proxy HA statistics summary.

```
diagnose sys sip-proxy stats ha
```

diagnose sys sip-proxy stats list

SIP proxy activity statistics.

```
diagnose sys sip-proxy stats list
```

diagnose sys sip-proxy stats mem

Memory usage.

```
diagnose sys sip-proxy stats mem
```

diagnose sys sip-proxy stats mem full

Memory usage details.

```
diagnose sys sip-proxy stats mem full
```

diagnose sys sip-proxy stats mem summary

Memory usage summary.

```
diagnose sys sip-proxy stats mem summary
```

diagnose sys sip-proxy stats proto

SIP proxy general protocol statistics summary.

```
diagnose sys sip-proxy stats proto
```

diagnose sys sip-proxy stats ssl-auth

SIP proxy SSL authentication statistics.

```
diagnose sys sip-proxy stats ssl-auth
```

diagnose sys sip-proxy stats udp

SIP proxy UDP statistics summary.

```
diagnose sys sip-proxy stats udp
```

diagnose sys sip-proxy valgrind

Valgrind analysis.

```
diagnose sys sip-proxy valgrind
```

diagnose sys sip-proxy valgrind disable

Force daemon to restart.

```
diagnose sys sip-proxy valgrind disable
```

diagnose sys sip-proxy valgrind enable

Force daemon to restart.

```
diagnose sys sip-proxy valgrind enable
```

diagnose sys sip-proxy valgrind log

Valgrind logs.

```
diagnose sys sip-proxy valgrind log
```

diagnose sys sip-proxy valgrind log clear

Clear logs.

```
diagnose sys sip-proxy valgrind log clear
```

diagnose sys sip-proxy valgrind log show

Show logs.

```
diagnose sys sip-proxy valgrind log show
```

diagnose sys sip-proxy valgrind memcheck

Force daemon to restart.

```
diagnose sys sip-proxy valgrind memcheck
```

diagnose sys sip-proxy valgrind memcheck_less

Force daemon to restart.

```
diagnose sys sip-proxy valgrind memcheck_less
```

diagnose sys sip-proxy valgrind status

Show valgrind status.

```
diagnose sys sip-proxy valgrind status
```

diagnose sys sip-proxy vdom

Diagnostics for VDOM in VoIP Daemon.

```
diagnose sys sip-proxy vdom
```

diagnose sys sip-proxy vdom list

List active VDOMs in VoIP daemon.

```
diagnose sys sip-proxy vdom list
```


diagnose sys sip-proxy vip

VIPs

```
diagnose sys sip-proxy vip
```

diagnose sys sip-proxy vip real-server

Real server VIP list.

```
diagnose sys sip-proxy vip real-server
```

diagnose sys speedtest-server

speed test server.

```
diagnose sys speedtest-server
```

diagnose sys speedtest-server clients

Speed test clients.

```
diagnose sys speedtest-server clients
```

diagnose sys speedtest-server clients flush

Flush pending speed test clients.

```
diagnose sys speedtest-server clients flush
```

diagnose sys speedtest-server clients list

List pending speed test clients.

```
diagnose sys speedtest-server clients list
```

diagnose sys speedtest-server controller

Speed test controller

```
diagnose sys speedtest-server controller
```

diagnose sys speedtest-server controller add

Add a controller

```
diagnose sys speedtest-server controller add <interface>
```

Parameter	Description	Type	Size
<interface>	Name of the interface.	string	

diagnose sys speedtest-server controller del

Delete a controller

```
diagnose sys speedtest-server controller del <interface>
```

Parameter	Description	Type	Size
<interface>	Name of the interface.	string	

diagnose sys speedtest-server controller list

List controllers.

```
diagnose sys speedtest-server controller list <name>
```

Parameter	Description	Type	Size
<name>	Name of the controller.	string	

diagnose sys speedtest-server log

Speed test result log.

```
diagnose sys speedtest-server log
```

diagnose sys speedtest-server log del-file

Delete log file.

```
diagnose sys speedtest-server log del-file
```

diagnose sys speedtest-server log list

List result log cache.

```
diagnose sys speedtest-server log list
```

diagnose sys speedtest-server log load-disk

Load log file to memory.

```
diagnose sys speedtest-server log load-disk
```

diagnose sys speedtest-server log save-disk

Save result logs to file.

```
diagnose sys speedtest-server log save-disk
```

diagnose sys speedtest-server speedtest-dbg

Toggle speed test debug output

```
diagnose sys speedtest-server speedtest-dbg
```

diagnose sys tcp-auth-options

TCP auth options info.

```
diagnose sys tcp-auth-options
```

diagnose sys tcp-option

Enable/disable TCP option.

```
diagnose sys tcp-option
```

diagnose sys tcp-option dump

Show TCP option status

```
diagnose sys tcp-option dump
```

diagnose sys tcp-option sack

Enable/disable sack.

```
diagnose sys tcp-option sack
```

diagnose sys tcp-option sack disable

disable

```
diagnose sys tcp-option sack disable
```

diagnose sys tcp-option sack enable

enable

```
diagnose sys tcp-option sack enable
```

diagnose sys tcp-option timestamps

Enable/disable timestamps.

```
diagnose sys tcp-option timestamps
```

diagnose sys tcp-option timestamps disable

disable

```
diagnose sys tcp-option timestamps disable
```

diagnose sys tcp-option timestamps enable

enable

```
diagnose sys tcp-option timestamps enable
```

diagnose sys tcp-option window-scale

Enable/disable window scale.

```
diagnose sys tcp-option window-scale
```

diagnose sys tcp-option window-scale disable

disable

```
diagnose sys tcp-option window-scale disable
```

diagnose sys tcp-option window-scale enable

enable

```
diagnose sys tcp-option window-scale enable
```

diagnose sys tcpsock

TCP sock info.

```
diagnose sys tcpsock
```

diagnose sys tcpsock6

TCP sock6 info.

```
diagnose sys tcpsock6
```

diagnose sys top

Show top processes information.

```
diagnose sys top <value> <Integer> <value>
```

Parameter	Description	Type	Size
<value>	Delay in seconds (default 5).	string	
<Integer>	Maximum lines to display (default 20). Show all the running processes if larger than its total number.	string	
<value>	Iterations to run (default unlimited).	string	

diagnose sys top-all

Show top threads information.

```
diagnose sys top-all <value> <Integer> <value>
```

Parameter	Description	Type	Size
<value>	Delay in seconds (default 5).	string	
<Integer>	Maximum lines to display (default 20). Show all the running threads if larger than its total number.	string	
<value>	Iterations to run (default unlimited).	string	

diagnose sys top-fd

Display processes with the most active file descriptors (default 5 processes).

```
diagnose sys top-fd [process-count]
```

Parameter	Description	Type	Size
[process-count]	Number of processes to include info for (default 5).	string	

diagnose sys top-fd detail

Display per-process active fd info along with details (default 5 processes, 50 fds).

```
diagnose sys top-fd detail [process-count] [fd-count]
```

Parameter	Description	Type	Size
[process-count]	Number of processes to include info for (default 5).	string	
[fd-count]	Number of FDs to include (per process, default 50).	string	

diagnose sys top-mem

Display processes with the most used memory (default 5 processes).

```
diagnose sys top-mem [process-count]
```

Parameter	Description	Type	Size
[process-count]	Number of processes to include info for (default 5).	string	

diagnose sys top-mem detail

Display per-process memory info along with details (default 5 processes).

```
diagnose sys top-mem detail [process-count]
```

Parameter	Description	Type	Size
[process-count]	Number of processes to include info for (default 5).	string	

diagnose sys top-sockmem

Display processes with the most used socket memory (default 5 processes).

```
diagnose sys top-sockmem [process-count]
```

Parameter	Description	Type	Size
[process-count]	Number of processes to include info for (default 5).	string	

diagnose sys traffic

Traffic information

```
diagnose sys traffic
```

diagnose sys traffic app-stats

Traffic application statistics.

```
diagnose sys traffic app-stats
```

diagnose sys traffic app-stats add

Add traffic application statistics entry.

```
diagnose sys traffic app-stats add <app_id>
```

Parameter	Description	Type	Size
<app_id>	A decimal number.	string	

diagnose sys traffic app-stats del

Delete traffic application statistics entry.

```
diagnose sys traffic app-stats del <app_id>
```

Parameter	Description	Type	Size
<app_id>	A decimal number.	string	

diagnose sys traffic app-stats hash-stats

Traffic application hash statistics.

```
diagnose sys traffic app-stats hash-stats
```


diagnose sys traffic app-stats list

List traffic application statistics entry.

```
diagnose sys traffic app-stats list <app_id>
```

Parameter	Description	Type	Size
<app_id>	A decimal number.	string	

diagnose sys traffic statistics

Traffic statistics

```
diagnose sys traffic statistics
```

diagnose sys traffic statistics clear

Clear traffic stats.

```
diagnose sys traffic statistics clear
```

diagnose sys traffic statistics show

Show traffic stats.

```
diagnose sys traffic statistics show
```

diagnose sys traffic-priority

Traffic Priority (DSCP/TOS).

```
diagnose sys traffic-priority
```

diagnose sys traffic-priority list

List traffic priority settings.

```
diagnose sys traffic-priority list
```

diagnose sys udp-reserved-port

Reserved UDP ports.

```
diagnose sys udp-reserved-port
```

diagnose sys udp-reserved-port test

Test if port has been reserved.

```
diagnose sys udp-reserved-port test <port> [vdom]
```

Parameter	Description	Type	Size
<port>	UDP port that will be tested	string	
[vdom]	VDOM name. If not specified, global reserved UDP ports will be used to test	string	

diagnose sys udpsock

UDP sock info.

```
diagnose sys udpsock
```

diagnose sys udpsock6

UDP sock6 info.

```
diagnose sys udpsock6
```

diagnose sys upgrade-report

Upgrade reports.

```
diagnose sys upgrade-report
```

diagnose sys upgrade-report current

Display the stats currently.

```
diagnose sys upgrade-report current
```

diagnose sys upgrade-report generate

Generate upgrade report and replace the one on disk.

```
diagnose sys upgrade-report generate
```

diagnose sys upgrade-report on-disk

Display the stats saved on disk.

```
diagnose sys upgrade-report on-disk
```

diagnose sys uuid

UUID debug.

```
diagnose sys uuid
```

diagnose sys uuid allow-manual-set

Allow to set UUID manually.

```
diagnose sys uuid allow-manual-set
```

diagnose sys uuid allow-manual-set disable

Disable.

```
diagnose sys uuid allow-manual-set disable
```

diagnose sys uuid allow-manual-set enable

Enable.

```
diagnose sys uuid allow-manual-set enable
```

diagnose sys uuid generate

Generate a UUID.

```
diagnose sys uuid generate
```

diagnose sys var-zone

var-zone information.

```
diagnose sys var-zone
```

diagnose sys var-zone show

Show var-zone data.

```
diagnose sys var-zone show
```

diagnose sys vd

Virtual domain management.

```
diagnose sys vd
```

diagnose sys vd add

Add a Virtual System.

```
diagnose sys vd add <vdname>
```

Parameter	Description	Type	Size
<vdname>	Virtual Domain Name.	string	

diagnose sys vd delete

Delete a Virtual System.

```
diagnose sys vd delete <vdname>
```

Parameter	Description	Type	Size
<vdname>	Virtual Domain Name.	string	

diagnose sys vd list

List Virtual Domains.

```
diagnose sys vd list
```

diagnose sys vd set

Set current VDOM.

```
diagnose sys vd set <vdname>
```

Parameter	Description	Type	Size
<vdname>	Virtual Domain Name.	string	

diagnose sys vd stats

Show VDOM statistics.

```
diagnose sys vd stats
```

diagnose sys vdom-property

VDOM property information.

```
diagnose sys vdom-property
```

diagnose sys vlan

vlan

```
diagnose sys vlan
```

diagnose sys vlan list

List VLAN.

```
diagnose sys vlan list
```

diagnose sys vxlan

VXLAN diagnostics.

```
diagnose sys vxlan
```

diagnose sys vxlan device

VXLAN device.

```
diagnose sys vxlan device
```

diagnose sys vxlan device list

Display VXLAN devices.

```
diagnose sys vxlan device list
```

diagnose sys vxlan fdb

VXLAN forwarding DB.

```
diagnose sys vxlan fdb
```

diagnose sys vxlan fdb list

Display VXLAN forwarding DB.

```
diagnose sys vxlan fdb list <string>
```

Parameter	Description	Type	Size
<string>	Interface name.	string	

diagnose sys vxlan fdb stat

Display VXLAN forwarding DB statistics.

```
diagnose sys vxlan fdb stat <string>
```

Parameter	Description	Type	Size
<string>	Interface name.	string	

diagnose sys waninfo

Get WAN Information through FortiGuard.

```
diagnose sys waninfo
```

diagnose sys waninfo ipify

Get public IP through <https://api.ipify.org>.

```
diagnose sys waninfo ipify <ddd.ddd.ddd.ddd> or <interface name> <vdom>
```

Parameter	Description	Type	Size
<ddd.ddd.ddd.ddd> or <interface name>	Specify the source IPv4 address or interface name.	string	
<vdom>	Specify the Virtual Domain name.	string	

diagnose sys wccp

wccp

```
diagnose sys wccp
```

diagnose sys wccp delete

Delete one wccp service.

```
diagnose sys wccp delete <xxx>
```

Parameter	Description	Type	Size
<xxx>	Service ID.	string	

diagnose sys wccp flush

Flush wccp services.

```
diagnose sys wccp flush
```

diagnose sys wccp list

List wccp services.

```
diagnose sys wccp list
```

diagnose test analytics-pdf-report

Retrieve analytics PDF report from FortiSandbox.

This topic includes the following commands:

- [diagnose test analytics-pdf-report list on page 3336](#)
- [diagnose test analytics-pdf-report max on page 3336](#)
- [diagnose test analytics-pdf-report request on page 3337](#)
- [diagnose test analytics-pdf-report status on page 3337](#)

diagnose test analytics-pdf-report list

List the PDF report requested.

```
diagnose test analytics-pdf-report list
```

diagnose test analytics-pdf-report max

Maximum number of PDF reports to cache in this FortiGate (<1> - <100>, default = 10).

```
diagnose test analytics-pdf-report max
```


diagnose test analytics-pdf-report request

Send the checksum of file to download.

```
diagnose test analytics-pdf-report request
```

diagnose test analytics-pdf-report status

Send the checksum of file to query status.

```
diagnose test analytics-pdf-report status
```

diagnose test analytics-report

Retrieve analytics report from FortiSandbox.

This topic includes the following commands:

- [diagnose test analytics-report checksum on page 3337](#)

diagnose test analytics-report checksum

Checksum of file to query.

```
diagnose test analytics-report checksum
```

diagnose test application

application

This topic includes the following commands:

- [diagnose test application acd on page 3339](#)
- [diagnose test application acsd on page 3340](#)
- [diagnose test application autod on page 3340](#)
- [diagnose test application awsd on page 3340](#)
- [diagnose test application azd on page 3340](#)
- [diagnose test application bfd on page 3340](#)
- [diagnose test application cloudapid on page 3341](#)
- [diagnose test application cmdbsvr on page 3341](#)

- [diagnose test application csfd on page 3341](#)
- [diagnose test application ddnsd on page 3341](#)
- [diagnose test application dhcp6c on page 3342](#)
- [diagnose test application dhcp6r on page 3342](#)
- [diagnose test application dhcprelay on page 3342](#)
- [diagnose test application dlpfingerprint on page 3342](#)
- [diagnose test application dlpfpcache on page 3343](#)
- [diagnose test application dnsproxy on page 3343](#)
- [diagnose test application dsd on page 3343](#)
- [diagnose test application eap_supp on page 3343](#)
- [diagnose test application evpn on page 3344](#)
- [diagnose test application fas on page 3344](#)
- [diagnose test application fcnacd on page 3344](#)
- [diagnose test application fds_notify on page 3344](#)
- [diagnose test application fgtlogd on page 3344](#)
- [diagnose test application fnbamd on page 3345](#)
- [diagnose test application forticldd on page 3345](#)
- [diagnose test application forticron on page 3345](#)
- [diagnose test application fortimq on page 3345](#)
- [diagnose test application fsvrd on page 3346](#)
- [diagnose test application gcpcd on page 3346](#)
- [diagnose test application harelay on page 3346](#)
- [diagnose test application hasync on page 3346](#)
- [diagnose test application hatalk on page 3347](#)
- [diagnose test application ibmd on page 3347](#)
- [diagnose test application imap on page 3347](#)
- [diagnose test application init on page 3347](#)
- [diagnose test application iotd on page 3347](#)
- [diagnose test application ipamd on page 3348](#)
- [diagnose test application ipamsd on page 3348](#)
- [diagnose test application ipldbd on page 3348](#)
- [diagnose test application ipsengine on page 3348](#)
- [diagnose test application ipsmonitor on page 3349](#)
- [diagnose test application ipsufd on page 3349](#)
- [diagnose test application kmipd on page 3349](#)
- [diagnose test application kubed on page 3349](#)
- [diagnose test application l2tpcd on page 3350](#)
- [diagnose test application lnkmttd on page 3350](#)
- [diagnose test application locallogd on page 3350](#)
- [diagnose test application miglogd on page 3350](#)
- [diagnose test application mrd on page 3351](#)
- [diagnose test application netxd on page 3351](#)
- [diagnose test application nntp on page 3351](#)

- [diagnose test application acid on page 3351](#)
- [diagnose test application openstackd on page 3352](#)
- [diagnose test application ovrd on page 3352](#)
- [diagnose test application pcpd on page 3352](#)
- [diagnose test application pop3 on page 3352](#)
- [diagnose test application pptpcd on page 3353](#)
- [diagnose test application quarantined on page 3353](#)
- [diagnose test application radius-das on page 3353](#)
- [diagnose test application radiusd on page 3353](#)
- [diagnose test application radvd on page 3354](#)
- [diagnose test application reportd on page 3354](#)
- [diagnose test application sdncd on page 3354](#)
- [diagnose test application sdnd on page 3354](#)
- [diagnose test application sepmd on page 3354](#)
- [diagnose test application sessionsync on page 3355](#)
- [diagnose test application sflowd on page 3355](#)
- [diagnose test application sfupgraded on page 3355](#)
- [diagnose test application smtp on page 3355](#)
- [diagnose test application snmpd on page 3356](#)
- [diagnose test application syslogd on page 3356](#)
- [diagnose test application updated on page 3356](#)
- [diagnose test application uploadd on page 3356](#)
- [diagnose test application urlfilter on page 3357](#)
- [diagnose test application vned on page 3357](#)
- [diagnose test application vrrp on page 3357](#)
- [diagnose test application waagent on page 3357](#)
- [diagnose test application wad on page 3358](#)
- [diagnose test application wccpd on page 3358](#)
- [diagnose test application wf_monitor on page 3358](#)
- [diagnose test application wiredapd on page 3358](#)
- [diagnose test application zebos_launcher on page 3359](#)

diagnose test application acid

Aggregate Controller.

```
diagnose test application acid <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application acsd

Ali Cloud Service daemon.

```
diagnose test application acsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application autod

Automation daemon.

```
diagnose test application autod <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application awsd

Amazon Web Services (AWS) daemon.

```
diagnose test application awsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application azd

Microsoft Azure daemon.

```
diagnose test application azd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application bfd

BFD daemon.

```
diagnose test application bfd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application cloudapid

Cloud service communication daemon.

```
diagnose test application cloudapid <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application cmdbsvr

cmdb server

```
diagnose test application cmdbsvr <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application csfd

Security Fabric daemon.

```
diagnose test application csfd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ddnsd

DDNS client daemon.

```
diagnose test application ddnsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application dhcp6c

DHCP6 client daemon.

```
diagnose test application dhcp6c <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application dhcp6r

DHCP6 relay daemon.

```
diagnose test application dhcp6r <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application dhcprelay

DHCP relay daemon.

```
diagnose test application dhcprelay <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application dlpfingerprint

DLP fingerprint daemon.

```
diagnose test application dlpfingerprint <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application dlpfpcache

DLP fingerprint cache daemon.

```
diagnose test application dlpfpcache <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application dnsproxy

DNS proxy.

```
diagnose test application dnsproxy <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	
<Integer>	Daemon index.	string	

diagnose test application dsd

DLP Statistics daemon.

```
diagnose test application dsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application eap_supp

EAP Supplicant daemon.

```
diagnose test application eap_supp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application evpn

EVPN daemon.

```
diagnose test application evpn <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application fas

FortiToken Cloud daemon.

```
diagnose test application fas <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application fcnacd

FortiClient NAC daemon.

```
diagnose test application fcnacd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application fds_notify

Update Notification daemon.

```
diagnose test application fds_notify <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application fgtlogd

Fgtlog daemon.


```
diagnose test application fgtlogd <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	
<Integer>	Daemon index.	string	

diagnose test application fnbamd

FortiGate non-blocking auth daemon.

```
diagnose test application fnbamd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application forticldd

FortiCloud daemon.

```
diagnose test application forticldd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application forticron

Forticron daemon.

```
diagnose test application forticron <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application fortimq

fortimq daemon.

```
diagnose test application fortimq <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application fsvrd

FortiService daemon.

```
diagnose test application fsvrd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application gcpd

Google Cloud Platform (GCP) daemon.

```
diagnose test application gcpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application harelay

HA relay daemon.

```
diagnose test application harelay <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application hasync

HA sync daemon.

```
diagnose test application hasync <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application hataalk

HA talk daemon.

```
diagnose test application hataalk <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ibmd

IBM Cloud Infrastructure daemon.

```
diagnose test application ibmd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application imap

IMAP proxy.

```
diagnose test application imap <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application init

init process.

```
diagnose test application init <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application iotd

IoT device info daemon.

```
diagnose test application iotd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ipamd

IP Address Management daemon.

```
diagnose test application ipamd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ipamsd

IPAM server daemon.

```
diagnose test application ipamsd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ipldbd

IP load balancing daemon.

```
diagnose test application ipldbd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ipsengine

IPS sensor.

```
diagnose test application ipsengine <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ipsmonitor

IPS monitor.

```
diagnose test application ipsmonitor <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ipsufd

IPS urlfilter daemon.

```
diagnose test application ipsufd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application kmipd

KMIP daemon.

```
diagnose test application kmipd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application kubed

Kubernetes daemon.

```
diagnose test application kubed <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application l2tpcd

L2TP client daemon.

```
diagnose test application l2tpcd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application lnkmttd

Link monitor daemon.

```
diagnose test application lnkmttd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application locallogd

Locallogd daemon.

```
diagnose test application locallogd <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	
<Integer>	Daemon index.	string	

diagnose test application miglogd

Miglog logging daemon.

```
diagnose test application miglogd <Integer> <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	
<Integer>	Daemon index.	string	

Parameter	Description	Type	Size
<Integer>	test level 26: 255 for all miglogds test level 31: 0 -- summary only, 1 -- each log summary, 2 -- log details test level 35: Replay log interval(default=100)	string	

diagnose test application mrd

Mobile router daemon.

```
diagnose test application mrd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application netxd

VMWare NetX service manager daemon.

```
diagnose test application netxd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application nntp

NNTP proxy.

```
diagnose test application nntp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ocid

Oracle Cloud Infrastructure.

```
diagnose test application ocid <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application openstackd

OpenStack SDN connector daemon.

```
diagnose test application openstackd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application ovrd

Override daemon.

```
diagnose test application ovrd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application pcpd

PCP server daemon.

```
diagnose test application pcpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application pop3

POP3 proxy.

```
diagnose test application pop3 <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application pptpcd

PPTP client.

```
diagnose test application pptpcd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application quarantined

Quarantine daemon.

```
diagnose test application quarantined <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	
<Integer>	Daemon index.	string	

diagnose test application radius-das

Radius-das daemon.

```
diagnose test application radius-das <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application radiusd

RADIUS daemon.

```
diagnose test application radiusd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application radvd

radvd daemon.

```
diagnose test application radvd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application reportd

Report daemon.

```
diagnose test application reportd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application sdncd

SDN Connector daemon.

```
diagnose test application sdncd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application sdnd

SDN connector daemon.

```
diagnose test application sdnd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application sepmd

Symantec Endpoint Protection Manager daemon.

```
diagnose test application sepmc <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application sessionsync

Session sync daemon.

```
diagnose test application sessionsync <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application sflowd

sFlow daemon.

```
diagnose test application sflowd <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	
<Integer>	Daemon index.	string	

diagnose test application sfupgraded

Security Fabric Upgrade daemon.

```
diagnose test application sfupgraded <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application smtp

SMTP proxy.

```
diagnose test application smtp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application snmpd

SNMP daemon.

```
diagnose test application snmpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application syslogd

Syslog daemon.

```
diagnose test application syslogd <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	
<Integer>	Daemon index.	string	

diagnose test application updated

Update daemon.

```
diagnose test application updated <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application uploadd

Upload daemon.

```
diagnose test application uploadd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application urlfilter

URL filter daemon.

```
diagnose test application urlfilter <Integer> <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	
<Integer>	Daemon index.	string	

diagnose test application vned

Virtual network enabler daemon.

```
diagnose test application vned <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application vrrp

VRRP daemon.

```
diagnose test application vrrp <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application waagent

waagent daemon.

```
diagnose test application waagent <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application wad

WAD related processes.

```
diagnose test application wad <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application wccpd

WCCP daemon.

```
diagnose test application wccpd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application wf_monitor

WF monitor.

```
diagnose test application wf_monitor <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application wiredapd

Wiredapd daemon.

```
diagnose test application wiredapd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application zebos_launcher

ZEBOS Launcher daemon.

```
diagnose test application zebos_launcher <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test authserver

Test authentication server.

This topic includes the following commands:

- [diagnose test authserver cert on page 3359](#)
- [diagnose test authserver ext-idp on page 3359](#)
- [diagnose test authserver ldap on page 3360](#)
- [diagnose test authserver ldap-digest on page 3360](#)
- [diagnose test authserver ldap-direct on page 3360](#)
- [diagnose test authserver ldap-search on page 3360](#)
- [diagnose test authserver local on page 3360](#)
- [diagnose test authserver pop3 on page 3360](#)
- [diagnose test authserver radius on page 3361](#)
- [diagnose test authserver radius-direct on page 3361](#)
- [diagnose test authserver tacacs+ on page 3361](#)
- [diagnose test authserver tacacs+-direct on page 3361](#)
- [diagnose test authserver user on page 3361](#)

diagnose test authserver cert

Test certificate authentication.

```
diagnose test authserver cert
```

diagnose test authserver ext-idp

Test external identity provider.

```
diagnose test authserver ext-idp
```

diagnose test authserver ldap

Test LDAP server.

```
diagnose test authserver ldap
```

diagnose test authserver ldap-digest

Test LDAP HA1 password query.

```
diagnose test authserver ldap-digest
```

diagnose test authserver ldap-direct

Test LDAP server directly.

```
diagnose test authserver ldap-direct
```

diagnose test authserver ldap-search

Search LDAP server.

```
diagnose test authserver ldap-search
```

diagnose test authserver local

Test local user.

```
diagnose test authserver local
```

diagnose test authserver pop3

Test POP3 server.

```
diagnose test authserver pop3
```


diagnose test authserver radius

Test RADIUS server.

```
diagnose test authserver radius
```

diagnose test authserver radius-direct

Test RADIUS server directly.

```
diagnose test authserver radius-direct
```

diagnose test authserver tacacs+

test TACACS+ server.

```
diagnose test authserver tacacs+ <server_name> <username> <password>
```

Parameter	Description	Type	Size
<server_name>	Server name	string	
<username>	User name	string	
<password>	Pasword	string	

diagnose test authserver tacacs+-direct

Test TACACS+ server directly.

```
diagnose test authserver tacacs+-direct
```

diagnose test authserver user

Test user with group/user ID/name(s).

```
diagnose test authserver user
```

diagnose test guest

Guest user add/delete/list.

This topic includes the following commands:

- [diagnose test guest add on page 3362](#)
- [diagnose test guest del on page 3362](#)
- [diagnose test guest list on page 3362](#)

diagnose test guest add

Add a guest user.

```
diagnose test guest add
```

diagnose test guest del

Delete guest users.

```
diagnose test guest del
```

diagnose test guest list

List guest users.

```
diagnose test guest list
```

diagnose test scim

SCIM database queries.

This topic includes the following commands:

- [diagnose test scim get-group on page 3363](#)
- [diagnose test scim get-membership on page 3363](#)
- [diagnose test scim get-user on page 3363](#)
- [diagnose test scim list-clients on page 3363](#)
- [diagnose test scim list-groups on page 3363](#)
- [diagnose test scim list-users on page 3363](#)

diagnose test scim get-group

Get one group by client name and group name.

```
diagnose test scim get-group
```

diagnose test scim get-membership

Get membership by client name and user name.

```
diagnose test scim get-membership
```

diagnose test scim get-user

Get one user by client name and user name.

```
diagnose test scim get-user
```

diagnose test scim list-clients

List all clients in one vdom.

```
diagnose test scim list-clients
```

diagnose test scim list-groups

List all groups name belongs to client.

```
diagnose test scim list-groups
```

diagnose test scim list-users

List all users name belongs to client.

```
diagnose test scim list-users
```

diagnose test security

System security test.

This topic includes the following commands:

- [diagnose test security mount-invalid-flag on page 3364](#)
- [diagnose test security status on page 3364](#)

diagnose test security mount-invalid-flag

Test mounting with invalid flags.

```
diagnose test security mount-invalid-flag
```

diagnose test security status

Check system security enforcement status.

```
diagnose test security status
```

diagnose test update

Update daemon test.

This topic includes the following commands:

- [diagnose test update info on page 3364](#)
- [diagnose test update tzdb on page 3364](#)

diagnose test update info

Display debug info.

```
diagnose test update info
```

diagnose test update tzdb

Test TZDB.

```
diagnose test update tzdb
```

diagnose traffictest

Offloading traffic test using internal TX/RX

This topic includes the following commands:

- [diagnose traffictest client-intf on page 3365](#)
- [diagnose traffictest port on page 3365](#)
- [diagnose traffictest proto on page 3365](#)
- [diagnose traffictest proto 0 on page 3366](#)
- [diagnose traffictest proto 1 on page 3366](#)
- [diagnose traffictest run on page 3366](#)
- [diagnose traffictest server-intf on page 3367](#)
- [diagnose traffictest show on page 3367](#)

diagnose traffictest client-intf

Client interface.

```
diagnose traffictest client-intf <string>
```

Parameter	Description	Type	Size
<string>	Interface name	string	

diagnose traffictest port

TCP or UDP port number (1 - 65535).

```
diagnose traffictest port <port>
```

Parameter	Description	Type	Size
<port>	Port number	string	

diagnose traffictest proto

0 for TCP or 1 for UDP (default = 0).

```
diagnose traffictest proto
```

diagnose traffictest proto 0

TCP

```
diagnose traffictest proto 0
```

diagnose traffictest proto 1

UDP

```
diagnose traffictest proto 1
```

diagnose traffictest run

Start traffic.

```
diagnose traffictest run [-h/arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg] [arg]
```

Parameter	Description	Type	Size
[-h/arg]	Help/Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	

Parameter	Description	Type	Size
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	
[arg]	Multi-Arguments for client	string	

diagnose traffictest server-intf

Server interface.

```
diagnose traffictest server-intf <string>
```

Parameter	Description	Type	Size
<string>	Interface name	string	

diagnose traffictest show

Traffic settings show

```
diagnose traffictest show
```

diagnose user

User

This topic includes the following commands:

- [diagnose user banned-ip on page 3368](#)
- [diagnose user banned-ip add on page 3368](#)
- [diagnose user banned-ip add src4 on page 3368](#)
- [diagnose user banned-ip add src6 on page 3369](#)
- [diagnose user banned-ip clear on page 3369](#)
- [diagnose user banned-ip delete on page 3369](#)
- [diagnose user banned-ip delete src4 on page 3369](#)
- [diagnose user banned-ip delete src6 on page 3369](#)

- [diagnose user banned-ip list on page 3370](#)
- [diagnose user banned-ip list all on page 3370](#)
- [diagnose user banned-ip list src4 on page 3370](#)
- [diagnose user banned-ip list src6 on page 3370](#)
- [diagnose user banned-ip stat on page 3370](#)
- [diagnose user banned-ip stress-test on page 3370](#)
- [diagnose user device on page 3371](#)
- [diagnose user device clear on page 3371](#)
- [diagnose user device clear vd on page 3371](#)
- [diagnose user device del on page 3371](#)
- [diagnose user device get on page 3372](#)
- [diagnose user device list on page 3372](#)
- [diagnose user device list vd on page 3372](#)
- [diagnose user device stats on page 3372](#)

diagnose user banned-ip

Banned IP addresses.

```
diagnose user banned-ip
```

diagnose user banned-ip add

Add banned IP address.

```
diagnose user banned-ip add
```

diagnose user banned-ip add src4

IPv4 source ban.

```
diagnose user banned-ip add src4 <src-ipv4> <expiry> <ban-source> <creation-timestamp>
```

Parameter	Description	Type	Size
<src-ipv4>	Source IPv4 address.	string	
<expiry>	Expiry in seconds.	string	
<ban-source>	Ban source (admin/dlp/ips/av/dos/app).	string	
<creation-timestamp>	Optional, unix timestamp (seconds) for the creation date	string	

diagnose user banned-ip add src6

IPv6 source ban.

```
diagnose user banned-ip add src6 <src-ipv6> <expiry> <ban-source> <creation-timestamp>
```

Parameter	Description	Type	Size
<src-ipv6>	Source IPv6 address.	string	
<expiry>	Expiry in seconds.	string	
<ban-source>	Ban source (admin/dlp/ips/av/dos/app).	string	
<creation-timestamp>	Optional, unix timestamp (seconds) for the creation date	string	

diagnose user banned-ip clear

Clear all banned IP addresses.

```
diagnose user banned-ip clear
```

diagnose user banned-ip delete

Delete banned IP address.

```
diagnose user banned-ip delete
```

diagnose user banned-ip delete src4

IPv4 source ban.

```
diagnose user banned-ip delete src4 <src-ipv4>
```

Parameter	Description	Type	Size
<src-ipv4>	Source IPv4 address.	string	

diagnose user banned-ip delete src6

IPv6 source ban.

```
diagnose user banned-ip delete src6 <src-ipv6>
```

Parameter	Description	Type	Size
<src-ipv6>	Source IPv6 address.	string	

diagnose user banned-ip list

List banned IPs.

```
diagnose user banned-ip list
```

diagnose user banned-ip list all

List all bans.

```
diagnose user banned-ip list all
```

diagnose user banned-ip list src4

IPv4 source ban.

```
diagnose user banned-ip list src4
```

diagnose user banned-ip list src6

IPv6 source ban.

```
diagnose user banned-ip list src6
```

diagnose user banned-ip stat

stat

```
diagnose user banned-ip stat
```

diagnose user banned-ip stress-test

IPv4 stress test for SRC bans.

```
diagnose user banned-ip stress-test <ipv4> <expiry> <ban-counts> <ban-source>
```

Parameter	Description	Type	Size
<ipv4>	Starting IPv4 address.	string	
<expiry>	Expiry in seconds.	string	
<ban-counts>	Number of banned IP addresses.	string	
<ban-source>	Ban source (admin/dlp/ips/av/dos/app).	string	

diagnose user device

User devices.

```
diagnose user device
```

diagnose user device clear

Clear discovered hosts.

```
diagnose user device clear
```

diagnose user device clear vd

Clear discovered hosts in a specific virtual domain.

```
diagnose user device clear vd <name>
```

Parameter	Description	Type	Size
<name>	Virtual domain name to filter by.	string	

diagnose user device del

Remove a specific host.

```
diagnose user device del <mac>
```

Parameter	Description	Type	Size
<mac>	MAC address (xx:xx:xx:xx:xx:xx).	string	

diagnose user device get

List a specific host.

```
diagnose user device get <mac>
```

Parameter	Description	Type	Size
<mac>	MAC address (xx:xx:xx:xx:xx:xx).	string	

diagnose user device list

List known hosts.

```
diagnose user device list
```

diagnose user device list vd

List discovered hosts in a specific virtual domain.

```
diagnose user device list vd <name>
```

Parameter	Description	Type	Size
<name>	Virtual domain name to filter by.	string	

diagnose user device stats

User device stats.

```
diagnose user device stats
```

diagnose user-device-store

User device store diagnostics.

This topic includes the following commands:

- [diagnose user-device-store device on page 3374](#)
- [diagnose user-device-store device disk on page 3375](#)
- [diagnose user-device-store device disk clear on page 3375](#)

- [diagnose user-device-store device disk list on page 3375](#)
- [diagnose user-device-store device disk query on page 3375](#)
- [diagnose user-device-store device fortifone on page 3375](#)
- [diagnose user-device-store device fortifone add on page 3375](#)
- [diagnose user-device-store device fortifone delete on page 3376](#)
- [diagnose user-device-store device fortifone list on page 3376](#)
- [diagnose user-device-store device memory on page 3376](#)
- [diagnose user-device-store device memory list on page 3376](#)
- [diagnose user-device-store device memory mac-host on page 3376](#)
- [diagnose user-device-store device memory mac-host add on page 3376](#)
- [diagnose user-device-store device memory mac-host query on page 3377](#)
- [diagnose user-device-store device memory mac-host subscribe on page 3377](#)
- [diagnose user-device-store device memory mac-host subscribe disable on page 3377](#)
- [diagnose user-device-store device memory mac-host subscribe enable on page 3377](#)
- [diagnose user-device-store device memory mac-host validate on page 3377](#)
- [diagnose user-device-store device memory ot-purdue-set on page 3378](#)
- [diagnose user-device-store device memory query on page 3378](#)
- [diagnose user-device-store device memory uid on page 3378](#)
- [diagnose user-device-store device memory uid add on page 3378](#)
- [diagnose user-device-store device memory uid delete on page 3378](#)
- [diagnose user-device-store device memory uid update on page 3378](#)
- [diagnose user-device-store device memory vulnerability-clear on page 3379](#)
- [diagnose user-device-store device memory vulnerability-clear-all on page 3379](#)
- [diagnose user-device-store device memory vulnerability-detected on page 3379](#)
- [diagnose user-device-store device memory vulnerability-query on page 3379](#)
- [diagnose user-device-store device memory vulnerability-update on page 3379](#)
- [diagnose user-device-store device-stats-query on page 3380](#)
- [diagnose user-device-store device-stats-query filters-and on page 3380](#)
- [diagnose user-device-store device-stats-query filters-or on page 3380](#)
- [diagnose user-device-store email-stats on page 3380](#)
- [diagnose user-device-store email-stats list on page 3380](#)
- [diagnose user-device-store email-stats query on page 3380](#)
- [diagnose user-device-store fsw-device-stats-query on page 3381](#)
- [diagnose user-device-store fsw-device-stats-query filters-and on page 3381](#)
- [diagnose user-device-store fsw-device-stats-query filters-or on page 3381](#)
- [diagnose user-device-store ftcl-device-stats-query on page 3381](#)
- [diagnose user-device-store ftcl-device-stats-query filters-and on page 3381](#)
- [diagnose user-device-store ftcl-device-stats-query filters-or on page 3382](#)
- [diagnose user-device-store iot-ot-vuln on page 3382](#)
- [diagnose user-device-store iot-ot-vuln list on page 3382](#)
- [diagnose user-device-store iot-ot-vuln query on page 3382](#)
- [diagnose user-device-store unified on page 3382](#)
- [diagnose user-device-store unified clear on page 3382](#)

- [diagnose user-device-store unified debug on page 3383](#)
- [diagnose user-device-store unified debug disable on page 3383](#)
- [diagnose user-device-store unified debug enable on page 3383](#)
- [diagnose user-device-store unified delete on page 3383](#)
- [diagnose user-device-store unified device-memory-query on page 3383](#)
- [diagnose user-device-store unified device-memory-query filters-and on page 3383](#)
- [diagnose user-device-store unified device-memory-query filters-or on page 3384](#)
- [diagnose user-device-store unified device-query on page 3384](#)
- [diagnose user-device-store unified device-query filters-and on page 3384](#)
- [diagnose user-device-store unified device-query filters-or on page 3384](#)
- [diagnose user-device-store unified dump on page 3384](#)
- [diagnose user-device-store unified list on page 3384](#)
- [diagnose user-device-store unified re-query on page 3385](#)
- [diagnose user-device-store unified stats on page 3385](#)
- [diagnose user-device-store unified user-memory-query on page 3385](#)
- [diagnose user-device-store unified user-memory-query filters-and on page 3385](#)
- [diagnose user-device-store unified user-memory-query filters-or on page 3385](#)
- [diagnose user-device-store unified user-query on page 3385](#)
- [diagnose user-device-store unified user-query filters-and on page 3386](#)
- [diagnose user-device-store unified user-query filters-or on page 3386](#)
- [diagnose user-device-store user on page 3386](#)
- [diagnose user-device-store user disk on page 3386](#)
- [diagnose user-device-store user disk clear on page 3386](#)
- [diagnose user-device-store user disk list on page 3386](#)
- [diagnose user-device-store user disk query on page 3387](#)
- [diagnose user-device-store user memory on page 3387](#)
- [diagnose user-device-store user memory list on page 3387](#)
- [diagnose user-device-store user memory query on page 3387](#)
- [diagnose user-device-store user-count on page 3387](#)
- [diagnose user-device-store user-count list on page 3387](#)
- [diagnose user-device-store user-count query on page 3388](#)
- [diagnose user-device-store user-stats on page 3388](#)
- [diagnose user-device-store user-stats query on page 3388](#)

diagnose user-device-store device

Device sessions info.

```
diagnose user-device-store device
```

diagnose user-device-store device disk

On disk session info.

```
diagnose user-device-store device disk
```

diagnose user-device-store device disk clear

Clear all records.

```
diagnose user-device-store device disk clear
```

diagnose user-device-store device disk list

List all records.

```
diagnose user-device-store device disk list
```

diagnose user-device-store device disk query

Query by SQL WHERE clause.

```
diagnose user-device-store device disk query
```

diagnose user-device-store device fortifone

Add/Delete FortiFone information.

```
diagnose user-device-store device fortifone
```

diagnose user-device-store device fortifone add

Test add FortiFone device by <mac> <ip> <extension> <name>.

```
diagnose user-device-store device fortifone add
```

diagnose user-device-store device fortifone delete

Test deleting a FortiFone device by <mac> <ip>.

```
diagnose user-device-store device fortifone delete
```

diagnose user-device-store device fortifone list

List FortiFone devices.

```
diagnose user-device-store device fortifone list
```

diagnose user-device-store device memory

In memory sessions info.

```
diagnose user-device-store device memory
```

diagnose user-device-store device memory list

List all records.

```
diagnose user-device-store device memory list
```

diagnose user-device-store device memory mac-host

Query/Add/Subscribe/Validate Operations on mac host.

```
diagnose user-device-store device memory mac-host
```

diagnose user-device-store device memory mac-host add

Add by <vdom> <mac> <ip> <interface-name>.

```
diagnose user-device-store device memory mac-host add
```


diagnose user-device-store device memory mac-host query

Query mac host info by <vdom> <mac> [flags].

```
diagnose user-device-store device memory mac-host query
```

diagnose user-device-store device memory mac-host subscribe

Enable/disable subscribe to mac host notifications.

```
diagnose user-device-store device memory mac-host subscribe
```

diagnose user-device-store device memory mac-host subscribe disable

Disable subscribe for mac host notifications.

```
diagnose user-device-store device memory mac-host subscribe disable
```

diagnose user-device-store device memory mac-host subscribe enable

Enable subscribe for mac host notifications.

```
diagnose user-device-store device memory mac-host subscribe enable
```

diagnose user-device-store device memory mac-host validate

validate mac host with <vdom> <mac> <generation> [flags].

```
diagnose user-device-store device memory mac-host validate
```

diagnose user-device-store device memory ot-purdue-set

OT purdue level set.

```
diagnose user-device-store device memory ot-purdue-set
```

diagnose user-device-store device memory query

Query by <type> <op> <value1|value2|...

```
diagnose user-device-store device memory query
```

diagnose user-device-store device memory uid

In memory devices info with UID present.

```
diagnose user-device-store device memory uid
```

diagnose user-device-store device memory uid add

Test add UID devices by <count>.

```
diagnose user-device-store device memory uid add
```

diagnose user-device-store device memory uid delete

Test delete UID device by <uid> <mac> <ip>.

```
diagnose user-device-store device memory uid delete
```

diagnose user-device-store device memory uid update

Test update UID device by <uid> <tags-value-delimited-by-;>.

```
diagnose user-device-store device memory uid update
```

diagnose user-device-store device memory vulnerability-clear

Clear all IoT vulnerabilities.

```
diagnose user-device-store device memory vulnerability-clear
```

diagnose user-device-store device memory vulnerability-clear-all

Clear all IoT vulnerabilities of a device.

```
diagnose user-device-store device memory vulnerability-clear-all
```

diagnose user-device-store device memory vulnerability-detected

Notify user-store a OT/IOT device is detected.

```
diagnose user-device-store device memory vulnerability-detected
```

diagnose user-device-store device memory vulnerability-query

Query device vulnerability info by MAC and IP.

```
diagnose user-device-store device memory vulnerability-query
```

diagnose user-device-store device memory vulnerability-update

Notify user-store a OT/IOT device is detected and query FGD without looking up in cache.

```
diagnose user-device-store device memory vulnerability-update
```

diagnose user-device-store device-stats-query

Device stats.

```
diagnose user-device-store device-stats-query
```

diagnose user-device-store device-stats-query filters-and

Query by <stats-type> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store device-stats-query filters-and
```

diagnose user-device-store device-stats-query filters-or

Query by <stats-type> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store device-stats-query filters-or
```

diagnose user-device-store email-stats

Email stats.

```
diagnose user-device-store email-stats
```

diagnose user-device-store email-stats list

List all records.

```
diagnose user-device-store email-stats list
```

diagnose user-device-store email-stats query

Query by <type> <op> <value1|value2|...

```
diagnose user-device-store email-stats query
```

diagnose user-device-store fsw-device-stats-query

Fortiswitch Device stats.

```
diagnose user-device-store fsw-device-stats-query
```

diagnose user-device-store fsw-device-stats-query filters-and

Query by <stats-type> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store fsw-device-stats-query filters-and
```

diagnose user-device-store fsw-device-stats-query filters-or

Query by <stats-type> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store fsw-device-stats-query filters-or
```

diagnose user-device-store ftcl-device-stats-query

Forticlient Device stats.

```
diagnose user-device-store ftcl-device-stats-query
```

diagnose user-device-store ftcl-device-stats-query filters-and

Query by <stats-type> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store ftcl-device-stats-query filters-and
```

diagnose user-device-store ftcl-device-stats-query filters-or

Query by <stats-type> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store ftcl-device-stats-query filters-or
```

diagnose user-device-store iot-ot-vuln

IoT/OT Vulnerabilities.

```
diagnose user-device-store iot-ot-vuln
```

diagnose user-device-store iot-ot-vuln list

List all records.

```
diagnose user-device-store iot-ot-vuln list
```

diagnose user-device-store iot-ot-vuln query

Query by <type> <op> <value1|value2|...>

```
diagnose user-device-store iot-ot-vuln query
```

diagnose user-device-store unified

Unified queries info.

```
diagnose user-device-store unified
```

diagnose user-device-store unified clear

Delete all unified queries.

```
diagnose user-device-store unified clear
```

diagnose user-device-store unified debug

Enable/Disable debug logs for unified queries.

```
diagnose user-device-store unified debug
```

diagnose user-device-store unified debug disable

Disable debug logs for unified queries.

```
diagnose user-device-store unified debug disable
```

diagnose user-device-store unified debug enable

Enable debug logs for unified queries.

```
diagnose user-device-store unified debug enable
```

diagnose user-device-store unified delete

Delete unified query by <query-id>.

```
diagnose user-device-store unified delete
```

diagnose user-device-store unified device-memory-query

Get Device records along with associated User records from memory.

```
diagnose user-device-store unified device-memory-query
```

diagnose user-device-store unified device-memory-query filters-and

Query by <iteration-count> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store unified device-memory-query filters-and
```

diagnose user-device-store unified device-memory-query filters-or

Query by <iteration-count> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store unified device-memory-query filters-or
```

diagnose user-device-store unified device-query

Get Device records along with associated User records from memory and disk.

```
diagnose user-device-store unified device-query
```

diagnose user-device-store unified device-query filters-and

Query by <iteration-count> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store unified device-query filters-and
```

diagnose user-device-store unified device-query filters-or

Query by <iteration-count> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store unified device-query filters-or
```

diagnose user-device-store unified dump

Dump unified query stats by <query-id>.

```
diagnose user-device-store unified dump
```

diagnose user-device-store unified list

List unified queries.


```
diagnose user-device-store unified list
```

diagnose user-device-store unified re-query

Retrieve Query by <query-id> <iteration-start> <iteration-count>

```
diagnose user-device-store unified re-query
```

diagnose user-device-store unified stats

Get Stats for unified queries.

```
diagnose user-device-store unified stats
```

diagnose user-device-store unified user-memory-query

Get User records along with associated Device records from memory.

```
diagnose user-device-store unified user-memory-query
```

diagnose user-device-store unified user-memory-query filters-and

Query by <iteration-count> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store unified user-memory-query filters-and
```

diagnose user-device-store unified user-memory-query filters-or

Query by <iteration-count> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store unified user-memory-query filters-or
```

diagnose user-device-store unified user-query

Get User records along with associated Device records from memory and disk.

```
diagnose user-device-store unified user-query
```

diagnose user-device-store unified user-query filters-and

Query by <iteration-count> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store unified user-query filters-and
```

diagnose user-device-store unified user-query filters-or

Query by <iteration-count> <start-time> <end-time> <type1;op1;values1-delimited-by-|;type2;op2;values2-delimited-by-|...>

```
diagnose user-device-store unified user-query filters-or
```

diagnose user-device-store user

User sessions info.

```
diagnose user-device-store user
```

diagnose user-device-store user disk

On disk session info.

```
diagnose user-device-store user disk
```

diagnose user-device-store user disk clear

Clear all records.

```
diagnose user-device-store user disk clear
```

diagnose user-device-store user disk list

List all records.

```
diagnose user-device-store user disk list
```

diagnose user-device-store user disk query

Query by SQL WHERE clause.

```
diagnose user-device-store user disk query
```

diagnose user-device-store user memory

In memory sessions info.

```
diagnose user-device-store user memory
```

diagnose user-device-store user memory list

List all records.

```
diagnose user-device-store user memory list
```

diagnose user-device-store user memory query

Query by <type> <op> <value1|value2|...>.

```
diagnose user-device-store user memory query
```

diagnose user-device-store user-count

User count info.

```
diagnose user-device-store user-count
```

diagnose user-device-store user-count list

List all group user count records.

```
diagnose user-device-store user-count list
```

diagnose user-device-store user-count query

Query by groupname <value>.

```
diagnose user-device-store user-count query
```

diagnose user-device-store user-stats

User stats.

```
diagnose user-device-store user-stats
```

diagnose user-device-store user-stats query

Query by <yyyy-mm-dd> <time-range days>

```
diagnose user-device-store user-stats query
```

diagnose vendor-mac

Vendor MAC Database.

This topic includes the following commands:

- [diagnose vendor-mac id on page 3388](#)
- [diagnose vendor-mac id-summary on page 3389](#)
- [diagnose vendor-mac info on page 3389](#)
- [diagnose vendor-mac match on page 3389](#)

diagnose vendor-mac id

Vendor MAC ID.

```
diagnose vendor-mac id <id>
```

Parameter	Description	Type	Size
<id>	Vendor MAC ID (a nonzero integer).	string	

diagnose vendor-mac id-summary

Vendor MAC ID summary.

```
diagnose vendor-mac id-summary <id>
```

Parameter	Description	Type	Size
<id>	Vendor MAC ID (a nonzero integer).	string	

diagnose vendor-mac info

MAC Address information.

```
diagnose vendor-mac info <xx:xx:xx:xx:xx:xx>
```

Parameter	Description	Type	Size
<xx:xx:xx:xx:xx:xx>	Service MAC address.	string	

diagnose vendor-mac match

Find Vendor MAC for a specific MAC address and mask.

```
diagnose vendor-mac match <xx:xx:xx:xx:xx:xx> <mask>
```

Parameter	Description	Type	Size
<xx:xx:xx:xx:xx:xx>	MAC address.	string	
<mask>	mask (0 - 48).	string	

diagnose vpn ike

IKE

This topic includes the following commands:

- [diagnose vpn ike admin on page 3392](#)
- [diagnose vpn ike config on page 3392](#)
- [diagnose vpn ike config list on page 3392](#)
- [diagnose vpn ike config list summary on page 3392](#)
- [diagnose vpn ike counts on page 3392](#)

- [diagnose vpn ike crash on page 3392](#)
- [diagnose vpn ike crypto on page 3393](#)
- [diagnose vpn ike crypto stats on page 3393](#)
- [diagnose vpn ike errors on page 3393](#)
- [diagnose vpn ike fragmentation-override on page 3393](#)
- [diagnose vpn ike gateway on page 3393](#)
- [diagnose vpn ike gateway clear on page 3393](#)
- [diagnose vpn ike gateway clear name on page 3394](#)
- [diagnose vpn ike gateway filter on page 3394](#)
- [diagnose vpn ike gateway filter clear on page 3394](#)
- [diagnose vpn ike gateway filter dst-port on page 3394](#)
- [diagnose vpn ike gateway filter ifindex on page 3394](#)
- [diagnose vpn ike gateway filter loc-addr4 on page 3395](#)
- [diagnose vpn ike gateway filter loc-addr6 on page 3395](#)
- [diagnose vpn ike gateway filter name on page 3395](#)
- [diagnose vpn ike gateway filter negate on page 3395](#)
- [diagnose vpn ike gateway filter negate dst-port on page 3396](#)
- [diagnose vpn ike gateway filter negate ifindex on page 3396](#)
- [diagnose vpn ike gateway filter negate loc-addr4 on page 3396](#)
- [diagnose vpn ike gateway filter negate loc-addr6 on page 3396](#)
- [diagnose vpn ike gateway filter negate name on page 3396](#)
- [diagnose vpn ike gateway filter negate rem-addr4 on page 3396](#)
- [diagnose vpn ike gateway filter negate rem-addr6 on page 3397](#)
- [diagnose vpn ike gateway filter negate vd on page 3397](#)
- [diagnose vpn ike gateway filter rem-addr4 on page 3397](#)
- [diagnose vpn ike gateway filter rem-addr6 on page 3397](#)
- [diagnose vpn ike gateway filter vd on page 3397](#)
- [diagnose vpn ike gateway flush on page 3398](#)
- [diagnose vpn ike gateway flush name on page 3398](#)
- [diagnose vpn ike gateway list on page 3398](#)
- [diagnose vpn ike gateway list name on page 3398](#)
- [diagnose vpn ike ikev2-cookie-enforce on page 3398](#)
- [diagnose vpn ike log on page 3399](#)
- [diagnose vpn ike log filter on page 3399](#)
- [diagnose vpn ike log filter clear on page 3399](#)
- [diagnose vpn ike log filter dst-port on page 3399](#)
- [diagnose vpn ike log filter ifindex on page 3399](#)
- [diagnose vpn ike log filter list on page 3400](#)
- [diagnose vpn ike log filter loc-addr4 on page 3400](#)
- [diagnose vpn ike log filter loc-addr6 on page 3400](#)
- [diagnose vpn ike log filter mloc-addr4 on page 3400](#)
- [diagnose vpn ike log filter mloc-addr6 on page 3401](#)
- [diagnose vpn ike log filter mrem-addr4 on page 3401](#)

- [diagnose vpn ike log filter mrem-addr6 on page 3402](#)
- [diagnose vpn ike log filter name on page 3403](#)
- [diagnose vpn ike log filter negate on page 3403](#)
- [diagnose vpn ike log filter negate dst-port on page 3403](#)
- [diagnose vpn ike log filter negate ifindex on page 3403](#)
- [diagnose vpn ike log filter negate loc-addr4 on page 3403](#)
- [diagnose vpn ike log filter negate loc-addr6 on page 3403](#)
- [diagnose vpn ike log filter negate mloc-addr4 on page 3404](#)
- [diagnose vpn ike log filter negate mloc-addr6 on page 3404](#)
- [diagnose vpn ike log filter negate mrem-addr4 on page 3404](#)
- [diagnose vpn ike log filter negate mrem-addr6 on page 3404](#)
- [diagnose vpn ike log filter negate name on page 3404](#)
- [diagnose vpn ike log filter negate rem-addr4 on page 3404](#)
- [diagnose vpn ike log filter negate rem-addr6 on page 3405](#)
- [diagnose vpn ike log filter negate vd on page 3405](#)
- [diagnose vpn ike log filter rem-addr4 on page 3405](#)
- [diagnose vpn ike log filter rem-addr6 on page 3405](#)
- [diagnose vpn ike log filter vd on page 3405](#)
- [diagnose vpn ike log function-name on page 3406](#)
- [diagnose vpn ike log function-name disable on page 3406](#)
- [diagnose vpn ike log function-name enable on page 3406](#)
- [diagnose vpn ike log terminal on page 3406](#)
- [diagnose vpn ike log terminal clear on page 3406](#)
- [diagnose vpn ike log terminal reset on page 3406](#)
- [diagnose vpn ike log terminal stats on page 3407](#)
- [diagnose vpn ike manager on page 3407](#)
- [diagnose vpn ike qkd on page 3407](#)
- [diagnose vpn ike restart on page 3407](#)
- [diagnose vpn ike routes on page 3407](#)
- [diagnose vpn ike routes list on page 3407](#)
- [diagnose vpn ike secrets on page 3408](#)
- [diagnose vpn ike stats on page 3408](#)
- [diagnose vpn ike status on page 3408](#)
- [diagnose vpn ike status detailed on page 3408](#)
- [diagnose vpn ike status summary on page 3408](#)
- [diagnose vpn ike valgrind on page 3408](#)
- [diagnose vpn ike valgrind disable on page 3409](#)
- [diagnose vpn ike valgrind enable on page 3409](#)
- [diagnose vpn ike valgrind log on page 3409](#)
- [diagnose vpn ike valgrind log clear on page 3409](#)
- [diagnose vpn ike valgrind log show on page 3409](#)
- [diagnose vpn ike valgrind memcheck on page 3409](#)
- [diagnose vpn ike valgrind memcheck_less on page 3410](#)

- [diagnose vpn ike valgrind status on page 3410](#)

diagnose vpn ike admin

IKE admin statistics.

```
diagnose vpn ike admin
```

diagnose vpn ike config

IKE configuration.

```
diagnose vpn ike config
```

diagnose vpn ike config list

List IKE configuration.

```
diagnose vpn ike config list
```

diagnose vpn ike config list summary

List IKE configuration summary.

```
diagnose vpn ike config list summary
```

diagnose vpn ike counts

IKE object counts.

```
diagnose vpn ike counts
```

diagnose vpn ike crash

IKE crash statistics.

```
diagnose vpn ike crash
```


diagnose vpn ike crypto

IKE crypto diagnostics.

```
diagnose vpn ike crypto
```

diagnose vpn ike crypto stats

IKE crypto statistics.

```
diagnose vpn ike crypto stats
```

diagnose vpn ike errors

IKE statistics.

```
diagnose vpn ike errors
```

diagnose vpn ike fragmentation-override

Override IKE fragmentation.

```
diagnose vpn ike fragmentation-override <flags>
```

Parameter	Description	Type	Size
<flags>	Bitmask of fragmentation override flags.	string	

diagnose vpn ike gateway

IKE gateways.

```
diagnose vpn ike gateway
```

diagnose vpn ike gateway clear

Clear IKE gateways.

```
diagnose vpn ike gateway clear
```

diagnose vpn ike gateway clear name

Clear gateway by name.

```
diagnose vpn ike gateway clear name <name>
```

Parameter	Description	Type	Size
<name>	Name of IKE gateway to clear.	string	

diagnose vpn ike gateway filter

IKE filter.

```
diagnose vpn ike gateway filter
```

diagnose vpn ike gateway filter clear

Erase the current filter.

```
diagnose vpn ike gateway filter clear
```

diagnose vpn ike gateway filter dst-port

Destination port range to filter by.

```
diagnose vpn ike gateway filter dst-port <port>
```

Parameter	Description	Type	Size
<port>	Destination port.	string	

diagnose vpn ike gateway filter ifindex

Index of the interface that IKE connection is negotiated over.

```
diagnose vpn ike gateway filter ifindex <index>
```

Parameter	Description	Type	Size
<index>	Interface index, 0 matches all.	string	

diagnose vpn ike gateway filter loc-addr4

IPv4 local gateway address range to filter by.

```
diagnose vpn ike gateway filter loc-addr4 <ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Local gateway IPv4 address (from).	string	
<ipv4-address>	Local gateway IPv4 address (to).	string	

diagnose vpn ike gateway filter loc-addr6

IPv6 local gateway address range to filter by.

```
diagnose vpn ike gateway filter loc-addr6 <ipv6-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Local gateway IPv6 address (from).	string	
<ipv4-address>	Local gateway IPv6 address (to).	string	

diagnose vpn ike gateway filter name

Phase1 name to filter by.

```
diagnose vpn ike gateway filter name <name>
```

Parameter	Description	Type	Size
<name>	Name to filter by.	string	

diagnose vpn ike gateway filter negate

Negate existing setting of the specified filter parameter.

```
diagnose vpn ike gateway filter negate
```

diagnose vpn ike gateway filter negate dst-port

Negate destination port.

```
diagnose vpn ike gateway filter negate dst-port
```

diagnose vpn ike gateway filter negate ifindex

Negate interface index.

```
diagnose vpn ike gateway filter negate ifindex
```

diagnose vpn ike gateway filter negate loc-addr4

Negate IPv4 local gateway address.

```
diagnose vpn ike gateway filter negate loc-addr4
```

diagnose vpn ike gateway filter negate loc-addr6

Negate IPv6 local gateway address.

```
diagnose vpn ike gateway filter negate loc-addr6
```

diagnose vpn ike gateway filter negate name

Negate name.

```
diagnose vpn ike gateway filter negate name
```

diagnose vpn ike gateway filter negate rem-addr4

Negate IPv4 remote gateway address.

```
diagnose vpn ike gateway filter negate rem-addr4
```

diagnose vpn ike gateway filter negate rem-addr6

Negate IPv6 remote gateway address.

```
diagnose vpn ike gateway filter negate rem-addr6
```

diagnose vpn ike gateway filter negate vd

Negate virtual domain.

```
diagnose vpn ike gateway filter negate vd
```

diagnose vpn ike gateway filter rem-addr4

IPv4 remote gateway address range to filter by.

```
diagnose vpn ike gateway filter rem-addr4 <ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Remote gateway IPv4 address (from).	string	
<ipv4-address>	Remote gateway IPv4 address (to).	string	

diagnose vpn ike gateway filter rem-addr6

IPv6 remote gateway address range to filter by.

```
diagnose vpn ike gateway filter rem-addr6 <ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Remote gateway IPv6 address (from).	string	
<ipv6-address>	Remote gateway IPv6 address (to).	string	

diagnose vpn ike gateway filter vd

Index of virtual domain. -1 matches all.

```
diagnose vpn ike gateway filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose vpn ike gateway flush

Synonym for clear.

```
diagnose vpn ike gateway flush
```

diagnose vpn ike gateway flush name

Clear gateway by name.

```
diagnose vpn ike gateway flush name <name>
```

Parameter	Description	Type	Size
<name>	Name of IKE gateway to clear.	string	

diagnose vpn ike gateway list

list

```
diagnose vpn ike gateway list
```

diagnose vpn ike gateway list name

List gateway by name.

```
diagnose vpn ike gateway list name <name>
```

Parameter	Description	Type	Size
<name>	Name of IKE gateway to list.	string	

diagnose vpn ike ikev2-cookie-enforce

Set IKEv2 SA_INIT cookie enforcement.

```
diagnose vpn ike ikev2-cookie-enforce <enforce>
```

Parameter	Description	Type	Size
<enforce>	Enable/Disable responder IKEv2 cookie.	string	

diagnose vpn ike log

IKE debug log.

```
diagnose vpn ike log
```

diagnose vpn ike log filter

IKE debug log filter.

```
diagnose vpn ike log filter
```

diagnose vpn ike log filter clear

Erase the current filter.

```
diagnose vpn ike log filter clear
```

diagnose vpn ike log filter dst-port

Destination port range to filter by.

```
diagnose vpn ike log filter dst-port <port>
```

Parameter	Description	Type	Size
<port>	Destination port.	string	

diagnose vpn ike log filter ifindex

Index of the interface that IKE connection is negotiated over.

```
diagnose vpn ike log filter ifindex <index>
```

Parameter	Description	Type	Size
<index>	Interface index, 0 matches all.	string	

diagnose vpn ike log filter list

Display the current filter.

```
diagnose vpn ike log filter list
```

diagnose vpn ike log filter loc-addr4

IPv4 local gateway address range to filter by.

```
diagnose vpn ike log filter loc-addr4 <ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Local gateway IPv4 address (from).	string	
<ipv4-address>	Local gateway IPv4 address (to).	string	

diagnose vpn ike log filter loc-addr6

IPv6 local gateway address range to filter by.

```
diagnose vpn ike log filter loc-addr6 <ipv6-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Local gateway IPv6 address (from).	string	
<ipv4-address>	Local gateway IPv6 address (to).	string	

diagnose vpn ike log filter mloc-addr4

Multiple IPv4 local gateway address to filter by.

```
diagnose vpn ike log filter mloc-addr4 <ipv4-address> <ipv4-address> <ipv4-address> <ipv4-address>  
<ipv4-address> <ipv4-address>
```


Parameter	Description	Type	Size
<ipv4-address>	Local gateway IPv4 address 1, up to 6 IP addresses	string	
<ipv4-address>	Local gateway IPv4 address 2, up to 6 IP addresses	string	
<ipv4-address>	Local gateway IPv4 address 3, up to 6 IP addresses	string	
<ipv4-address>	Local gateway IPv4 address 4, up to 6 IP addresses	string	
<ipv4-address>	Local gateway IPv4 address 5, up to 6 IP addresses	string	
<ipv4-address>	Local gateway IPv4 address 6, up to 6 IP addresses	string	

diagnose vpn ike log filter mloc-addr6

Multiple IPv6 local gateway address to filter by.

```
diagnose vpn ike log filter mloc-addr6 <ipv6-address> <ipv6-address> <ipv6-address> <ipv6-address>  
<ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Local gateway IPv6 address 1, up to 6 IP addresses	string	
<ipv6-address>	Local gateway IPv6 address 2, up to 6 IP addresses	string	
<ipv6-address>	Local gateway IPv6 address 3, up to 6 IP addresses	string	
<ipv6-address>	Local gateway IPv6 address 4, up to 6 IP addresses	string	
<ipv6-address>	Local gateway IPv6 address 5, up to 6 IP addresses	string	
<ipv6-address>	Local gateway IPv6 address 6, up to 6 IP addresses	string	

diagnose vpn ike log filter mrem-addr4

Multiple IPv4 remote gateway address to filter by.

```
diagnose vpn ike log filter mrem-addr4 <ipv4-address> <ipv4-address> <ipv4-address> <ipv4-address>
<ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Remote gateway IPv4 address 1, up to 6 IP addresses	string	
<ipv4-address>	Remote gateway IPv4 address 2, up to 6 IP addresses	string	
<ipv4-address>	Remote gateway IPv4 address 3, up to 6 IP addresses	string	
<ipv4-address>	Remote gateway IPv4 address 4, up to 6 IP addresses	string	
<ipv4-address>	Remote gateway IPv4 address 5, up to 6 IP addresses	string	
<ipv4-address>	Remote gateway IPv4 address 6, up to 6 IP addresses	string	

diagnose vpn ike log filter mrem-addr6

Multiple IPv6 remote gateway addresses to filter by.

```
diagnose vpn ike log filter mrem-addr6 <ipv6-address> <ipv6-address> <ipv6-address> <ipv6-address>
<ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Remote gateway IPv6 address 1, up to 6 IP addresses	string	
<ipv6-address>	Remote gateway IPv6 address 2, up to 6 IP addresses	string	
<ipv6-address>	Remote gateway IPv6 address 3, up to 6 IP addresses	string	
<ipv6-address>	Remote gateway IPv6 address 4, up to 6 IP addresses	string	
<ipv6-address>	Remote gateway IPv6 address 5, up to 6 IP addresses	string	
<ipv6-address>	Remote gateway IPv6 address 6, up to 6 IP addresses	string	

diagnose vpn ike log filter name

Phase1 name to filter by.

```
diagnose vpn ike log filter name <name>
```

Parameter	Description	Type	Size
<name>	Name to filter by.	string	

diagnose vpn ike log filter negate

Negate existing setting of the specified filter parameter.

```
diagnose vpn ike log filter negate
```

diagnose vpn ike log filter negate dst-port

Negate destination port.

```
diagnose vpn ike log filter negate dst-port
```

diagnose vpn ike log filter negate ifindex

Negate interface index.

```
diagnose vpn ike log filter negate ifindex
```

diagnose vpn ike log filter negate loc-addr4

Negate IPv4 local gateway address.

```
diagnose vpn ike log filter negate loc-addr4
```

diagnose vpn ike log filter negate loc-addr6

Negate IPv6 local gateway address.

```
diagnose vpn ike log filter negate loc-addr6
```

diagnose vpn ike log filter negate mloc-addr4

Negate multiple IPv4 local gateway addresses.

```
diagnose vpn ike log filter negate mloc-addr4
```

diagnose vpn ike log filter negate mloc-addr6

Negate multiple IPv6 local gateway addresses.

```
diagnose vpn ike log filter negate mloc-addr6
```

diagnose vpn ike log filter negate mrem-addr4

Negate multiple IPv4 remote gateway addresses.

```
diagnose vpn ike log filter negate mrem-addr4
```

diagnose vpn ike log filter negate mrem-addr6

Negate multiple IPv6 remote gateway address.

```
diagnose vpn ike log filter negate mrem-addr6
```

diagnose vpn ike log filter negate name

Negate name.

```
diagnose vpn ike log filter negate name
```

diagnose vpn ike log filter negate rem-addr4

Negate IPv4 remote gateway address address.

```
diagnose vpn ike log filter negate rem-addr4
```

diagnose vpn ike log filter negate rem-addr6

Negate IPv6 remote gateway address.

```
diagnose vpn ike log filter negate rem-addr6
```

diagnose vpn ike log filter negate vd

Negate virtual domain.

```
diagnose vpn ike log filter negate vd
```

diagnose vpn ike log filter rem-addr4

IPv4 remote gateway address range to filter by.

```
diagnose vpn ike log filter rem-addr4 <ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	Remote gateway IPv4 address (from).	string	
<ipv4-address>	Remote gateway IPv4 address (to).	string	

diagnose vpn ike log filter rem-addr6

IPv6 remote gateway address range to filter by.

```
diagnose vpn ike log filter rem-addr6 <ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	Remote gateway IPv6 address (from).	string	
<ipv6-address>	Remote gateway IPv6 address (to).	string	

diagnose vpn ike log filter vd

Index of virtual domain. -1 matches all.

```
diagnose vpn ike log filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain. -1 matches all.	string	

diagnose vpn ike log function-name

Enable/disable display function name.

```
diagnose vpn ike log function-name
```

diagnose vpn ike log function-name disable

Disable display of function name.

```
diagnose vpn ike log function-name disable
```

diagnose vpn ike log function-name enable

Enable display of function name.

```
diagnose vpn ike log function-name enable
```

diagnose vpn ike log terminal

IKE debug log terminal statistics.

```
diagnose vpn ike log terminal
```

diagnose vpn ike log terminal clear

Clear IKE debug log terminals.

```
diagnose vpn ike log terminal clear
```

diagnose vpn ike log terminal reset

Reset IKE debug log terminals.

```
diagnose vpn ike log terminal reset
```

diagnose vpn ike log terminal stats

Show IKE debug log terminal statistics.

```
diagnose vpn ike log terminal stats
```

diagnose vpn ike manager

IKE manager statistics.

```
diagnose vpn ike manager
```

diagnose vpn ike qkd

IKE QKD statistics.

```
diagnose vpn ike qkd <QKD-name>
```

Parameter	Description	Type	Size
<QKD-name>	IKE QKD server name.	string	

diagnose vpn ike restart

Restart IKE.

```
diagnose vpn ike restart
```

diagnose vpn ike routes

IKE routes.

```
diagnose vpn ike routes
```

diagnose vpn ike routes list

List IKE routes.

```
diagnose vpn ike routes list
```

diagnose vpn ike secrets

IKE secrets statistics.

```
diagnose vpn ike secrets
```

diagnose vpn ike stats

IKE statistics.

```
diagnose vpn ike stats
```

diagnose vpn ike status

IKE status.

```
diagnose vpn ike status
```

diagnose vpn ike status detailed

Detailed status.

```
diagnose vpn ike status detailed
```

diagnose vpn ike status summary

Status summary.

```
diagnose vpn ike status summary
```

diagnose vpn ike valgrind

Valgrind analysis.

```
diagnose vpn ike valgrind
```


diagnose vpn ike valgrind disable

Force daemon to restart.

```
diagnose vpn ike valgrind disable
```

diagnose vpn ike valgrind enable

Force daemon to restart.

```
diagnose vpn ike valgrind enable
```

diagnose vpn ike valgrind log

Valgrind logs.

```
diagnose vpn ike valgrind log
```

diagnose vpn ike valgrind log clear

Clear logs.

```
diagnose vpn ike valgrind log clear
```

diagnose vpn ike valgrind log show

Show logs.

```
diagnose vpn ike valgrind log show
```

diagnose vpn ike valgrind memcheck

Force daemon to restart.

```
diagnose vpn ike valgrind memcheck
```

diagnose vpn ike valgrind memcheck_less

Force daemon to restart.

```
diagnose vpn ike valgrind memcheck_less
```

diagnose vpn ike valgrind status

Show valgrind status.

```
diagnose vpn ike valgrind status
```

diagnose vpn ikecrypt

Multiprocess IKE crypto daemon diagnostics.

This topic includes the following commands:

- [diagnose vpn ikecrypt info on page 3410](#)
- [diagnose vpn ikecrypt restart on page 3410](#)
- [diagnose vpn ikecrypt valgrind on page 3411](#)
- [diagnose vpn ikecrypt valgrind disable on page 3411](#)
- [diagnose vpn ikecrypt valgrind enable on page 3411](#)
- [diagnose vpn ikecrypt valgrind log on page 3411](#)
- [diagnose vpn ikecrypt valgrind log clear on page 3411](#)
- [diagnose vpn ikecrypt valgrind log show on page 3411](#)
- [diagnose vpn ikecrypt valgrind memcheck on page 3412](#)
- [diagnose vpn ikecrypt valgrind memcheck_less on page 3412](#)
- [diagnose vpn ikecrypt valgrind status on page 3412](#)

diagnose vpn ikecrypt info

Display ikecrypt daemon information.

```
diagnose vpn ikecrypt info
```

diagnose vpn ikecrypt restart

Restart the ikecrypt daemon.

```
diagnose vpn ikecrypt restart
```

diagnose vpn ikecrypt valgrind

Valgrind analysis.

```
diagnose vpn ikecrypt valgrind
```

diagnose vpn ikecrypt valgrind disable

Force daemon to restart.

```
diagnose vpn ikecrypt valgrind disable
```

diagnose vpn ikecrypt valgrind enable

Force daemon to restart.

```
diagnose vpn ikecrypt valgrind enable
```

diagnose vpn ikecrypt valgrind log

Valgrind logs.

```
diagnose vpn ikecrypt valgrind log
```

diagnose vpn ikecrypt valgrind log clear

Clear logs.

```
diagnose vpn ikecrypt valgrind log clear
```

diagnose vpn ikecrypt valgrind log show

Show logs.

```
diagnose vpn ikecrypt valgrind log show
```

diagnose vpn ikecrypt valgrind memcheck

Force daemon to restart.

```
diagnose vpn ikecrypt valgrind memcheck
```

diagnose vpn ikecrypt valgrind memcheck_less

Force daemon to restart.

```
diagnose vpn ikecrypt valgrind memcheck_less
```

diagnose vpn ikecrypt valgrind status

Show valgrind status.

```
diagnose vpn ikecrypt valgrind status
```

diagnose vpn ipsec

General IPsec.

This topic includes the following commands:

- [diagnose vpn ipsec cpu on page 3412](#)
- [diagnose vpn ipsec cpu clear on page 3412](#)
- [diagnose vpn ipsec status on page 3413](#)

diagnose vpn ipsec cpu

Actions for software crypto CPU distributions.

```
diagnose vpn ipsec cpu
```

diagnose vpn ipsec cpu clear

Clear the stats.

```
diagnose vpn ipsec cpu clear
```

diagnose vpn ipsec status

Show status of IPsec.

```
diagnose vpn ipsec status
```

diagnose vpn l2tp

VPN L2TP.

This topic includes the following commands:

- [diagnose vpn l2tp status on page 3413](#)
- [diagnose vpn l2tp tunnel on page 3413](#)

diagnose vpn l2tp status

Display L2TP status.

```
diagnose vpn l2tp status
```

diagnose vpn l2tp tunnel

List L2TP tunnels.

```
diagnose vpn l2tp tunnel <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	IPv4 address of the client (all if don't specify)	string	

diagnose vpn mr

Multicast routing.

This topic includes the following commands:

- [diagnose vpn mr add on page 3414](#)
- [diagnose vpn mr del on page 3414](#)

- [diagnose vpn mr list-addr on page 3414](#)
- [diagnose vpn mr list-dev on page 3415](#)
- [diagnose vpn mr list-tun on page 3415](#)

diagnose vpn mr add

Add a multicast route.

```
diagnose vpn mr add <device> <tunnel-id> <mgrp> <vrf>
```

Parameter	Description	Type	Size
<device>	Name of IPsec device.	string	
<tunnel-id>	IPsec tunnel id.	string	
<mgrp>	Multicast IP.	string	
<vrf>	VRF ID.	string	

diagnose vpn mr del

Delete multicast routes.

```
diagnose vpn mr del <device> <tunnel-id> <mgrp> <vrf>
```

Parameter	Description	Type	Size
<device>	Name of IPsec device.	string	
<tunnel-id>	IPsec tunnel id.	string	
<mgrp>	Multicast IP.	string	
<vrf>	VRF ID.	string	

diagnose vpn mr list-addr

List by multicast address.

```
diagnose vpn mr list-addr <device> <address> <vrf>
```

Parameter	Description	Type	Size
<device>	Name of IPsec device.	string	
<address>	Multicast address.	string	
<vrf>	VRF ID.	string	

diagnose vpn mr list-dev

List by device.

```
diagnose vpn mr list-dev <device>
```

Parameter	Description	Type	Size
<device>	Name of IPsec device.	string	

diagnose vpn mr list-tun

List by tunnel.

```
diagnose vpn mr list-tun <tunnel>
```

Parameter	Description	Type	Size
<tunnel>	Name of IPsec tunnel.	string	

diagnose vpn mr6

IPv6 multicast routing.

This topic includes the following commands:

- [diagnose vpn mr6 add on page 3415](#)
- [diagnose vpn mr6 del on page 3416](#)
- [diagnose vpn mr6 list-addr on page 3416](#)
- [diagnose vpn mr6 list-dev on page 3416](#)
- [diagnose vpn mr6 list-tun on page 3417](#)

diagnose vpn mr6 add

Add a multicast route.

```
diagnose vpn mr6 add <device> <tunnel-id> <mgrp> <vrf>
```

Parameter	Description	Type	Size
<device>	Name of IPsec device.	string	

Parameter	Description	Type	Size
<tunnel-id>	IPsec tunnel id.	string	
<mgrp>	Multicast IP.	string	
<vrf>	VRF ID.	string	

diagnose vpn mr6 del

Delete multicast routes.

```
diagnose vpn mr6 del <device> <tunnel-id> <mgrp> <vrf>
```

Parameter	Description	Type	Size
<device>	Name of IPsec device.	string	
<tunnel-id>	IPsec tunnel id.	string	
<mgrp>	Multicast IP.	string	
<vrf>	VRF ID.	string	

diagnose vpn mr6 list-addr

List by multicast address.

```
diagnose vpn mr6 list-addr <device> <address> <vrf>
```

Parameter	Description	Type	Size
<device>	Name of IPsec device.	string	
<address>	Multicast address.	string	
<vrf>	VRF ID.	string	

diagnose vpn mr6 list-dev

List by device.

```
diagnose vpn mr6 list-dev <device>
```

Parameter	Description	Type	Size
<device>	Name of IPsec device.	string	

diagnose vpn mr6 list-tun

List by tunnel.

```
diagnose vpn mr6 list-tun <tunnel>
```

Parameter	Description	Type	Size
<tunnel>	Name of IPsec tunnel.	string	

diagnose vpn pptp

VPN PPTP.

This topic includes the following commands:

- [diagnose vpn pptp status on page 3417](#)

diagnose vpn pptp status

Display PPTP status.

```
diagnose vpn pptp status
```

diagnose vpn ssl

Agentless VPN.

This topic includes the following commands:

- [diagnose vpn ssl app-session on page 3418](#)
- [diagnose vpn ssl blocklist on page 3418](#)
- [diagnose vpn ssl blocklist count on page 3419](#)
- [diagnose vpn ssl blocklist del on page 3419](#)
- [diagnose vpn ssl blocklist list on page 3419](#)
- [diagnose vpn ssl cmdb-cache-log on page 3419](#)
- [diagnose vpn ssl debug-filter on page 3420](#)
- [diagnose vpn ssl debug-filter clear on page 3420](#)
- [diagnose vpn ssl debug-filter list on page 3420](#)
- [diagnose vpn ssl debug-filter negate on page 3420](#)
- [diagnose vpn ssl debug-filter negate src-addr4 on page 3420](#)

- [diagnose vpn ssl debug-filter negate src-addr6 on page 3420](#)
- [diagnose vpn ssl debug-filter negate vd on page 3421](#)
- [diagnose vpn ssl debug-filter src-addr4 on page 3421](#)
- [diagnose vpn ssl debug-filter src-addr6 on page 3421](#)
- [diagnose vpn ssl debug-filter vd on page 3421](#)
- [diagnose vpn ssl dist-usr on page 3422](#)
- [diagnose vpn ssl dist-usr count on page 3422](#)
- [diagnose vpn ssl dist-usr del on page 3422](#)
- [diagnose vpn ssl dist-usr list on page 3422](#)
- [diagnose vpn ssl info on page 3423](#)
- [diagnose vpn ssl list on page 3423](#)
- [diagnose vpn ssl peer-name on page 3423](#)
- [diagnose vpn ssl peer-name count on page 3423](#)
- [diagnose vpn ssl peer-name del on page 3423](#)
- [diagnose vpn ssl peer-name list on page 3424](#)
- [diagnose vpn ssl saml-metadata on page 3424](#)
- [diagnose vpn ssl statistics on page 3424](#)
- [diagnose vpn ssl user-session on page 3424](#)
- [diagnose vpn ssl usr-chg on page 3425](#)
- [diagnose vpn ssl usr-chg count on page 3425](#)
- [diagnose vpn ssl usr-chg del on page 3425](#)
- [diagnose vpn ssl usr-chg list on page 3425](#)
- [diagnose vpn ssl web-mode-test on page 3426](#)

diagnose vpn ssl app-session

List all app session in db.

```
diagnose vpn ssl app-session <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display all app session for all VDOMs or given VDOM name or VDOM ID. Without argument, app session for current VDOM is shown.	string	

diagnose vpn ssl blocklist

Agentless VPN blocklist information

```
diagnose vpn ssl blocklist
```

diagnose vpn ssl blocklist count

Print counts of Agentless VPN blocklist

```
diagnose vpn ssl blocklist count <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display Agentless VPN blocklist entries count for all VDOMs, given VDOM name or VDOM ID. Without argument, count for current VDOM is shown.	string	

diagnose vpn ssl blocklist del

Del Agentless VPN blocklist

```
diagnose vpn ssl blocklist del <all|vfid|addr>
```

Parameter	Description	Type	Size
<all vfid addr>	Delete block list entries for all VDOMs, given VDOM ID or address.	string	

diagnose vpn ssl blocklist list

List Agentless VPN blocklist

```
diagnose vpn ssl blocklist list <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display Agentless VPN blocklist information for all VDOMs, given VDOM name or VDOM ID. Without argument, information for current VDOM is shown.	string	

diagnose vpn ssl cmdb-cache-log

Enable/disable Agentless VPN cmdb cache log.

```
diagnose vpn ssl cmdb-cache-log <enable>
```

Parameter	Description	Type	Size
<enable>	Enable Agentless VPN cmdb cache log. disable Disable Agentless VPN cmdb cache log.	string	

diagnose vpn ssl debug-filter

Agentless VPN debug message filter.

```
diagnose vpn ssl debug-filter
```

diagnose vpn ssl debug-filter clear

Erase the current filter.

```
diagnose vpn ssl debug-filter clear
```

diagnose vpn ssl debug-filter list

Display the current filter.

```
diagnose vpn ssl debug-filter list
```

diagnose vpn ssl debug-filter negate

Negate the specified filter parameter.

```
diagnose vpn ssl debug-filter negate
```

diagnose vpn ssl debug-filter negate src-addr4

IPv4 source address.

```
diagnose vpn ssl debug-filter negate src-addr4
```

diagnose vpn ssl debug-filter negate src-addr6

IPv6 source address.

```
diagnose vpn ssl debug-filter negate src-addr6
```

diagnose vpn ssl debug-filter negate vd

Virtual domain.

```
diagnose vpn ssl debug-filter negate vd
```

diagnose vpn ssl debug-filter src-addr4

IPv4 source address range.

```
diagnose vpn ssl debug-filter src-addr4 <ipv4-address> <ipv4-address>
```

Parameter	Description	Type	Size
<ipv4-address>	source IPv4 address (from)	string	
<ipv4-address>	source IPv4 address (to)	string	

diagnose vpn ssl debug-filter src-addr6

IPv6 source address range.

```
diagnose vpn ssl debug-filter src-addr6 <ipv6-address> <ipv6-address>
```

Parameter	Description	Type	Size
<ipv6-address>	source IPv6 address (from)	string	
<ipv6-address>	source IPv6 address (to)	string	

diagnose vpn ssl debug-filter vd

Name of virtual domain.

```
diagnose vpn ssl debug-filter vd <vdom name>
```

Parameter	Description	Type	Size
<vdom name>	Name of virtual domain.	string	

diagnose vpn ssl dist-usr

Agentless VPN distinct user information

```
diagnose vpn ssl dist-usr
```

diagnose vpn ssl dist-usr count

Print counts of Agentless VPN distinct user

```
diagnose vpn ssl dist-usr count <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display Agentless VPN distinct user count for all VDOMs, given VDOM name or VDOM ID. Without argument, count for current VDOM is shown.	string	

diagnose vpn ssl dist-usr del

Del Agentless VPN distinct user

```
diagnose vpn ssl dist-usr del <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Delete distinct user for all VDOMs, given VDOM name or VDOM ID.	string	

diagnose vpn ssl dist-usr list

List Agentless VPN distinct users

```
diagnose vpn ssl dist-usr list <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display Agentless VPN distinct user information for all VDOMs, given VDOM name or VDOM ID. Without argument, information for current VDOM is shown.	string	

diagnose vpn ssl info

Agentless VPN information

```
diagnose vpn ssl info <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display Agentless VPN information for all VDOMs, given VDOM name or VDOM ID. Without argument, information for current VDOM is shown.	string	

diagnose vpn ssl list

List current connections.

```
diagnose vpn ssl list
```

diagnose vpn ssl peer-name

Agentless VPN Peer information

```
diagnose vpn ssl peer-name
```

diagnose vpn ssl peer-name count

Print counts of Agentless VPN peer information

```
diagnose vpn ssl peer-name count
```

diagnose vpn ssl peer-name del

Del Agentless VPN peer information

```
diagnose vpn ssl peer-name del
```

diagnose vpn ssl peer-name list

List Agentless VPN peer information

```
diagnose vpn ssl peer-name list
```

diagnose vpn ssl saml-metadata

Display Agentless VPN SAML SP metadata for given SAML name.

```
diagnose vpn ssl saml-metadata <SAML name>
```

Parameter	Description	Type	Size
<SAML name>	Name of SAML user.	string	

diagnose vpn ssl statistics

Agentless VPN statistics

```
diagnose vpn ssl statistics <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display Agentless VPN statistics for all VDOMs or given VDOM name or VDOM ID. Without argument, statistics for current VDOM is shown.	string	

diagnose vpn ssl user-session

List all user session in db.

```
diagnose vpn ssl user-session <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display all user session for all VDOMs or given VDOM name or VDOM ID. Without argument, user session for current VDOM is shown.	string	

diagnose vpn ssl usr-chg

Agentless VPN user information with password modification

```
diagnose vpn ssl usr-chg
```

diagnose vpn ssl usr-chg count

Print counts of Agentless VPN user change information

```
diagnose vpn ssl usr-chg count <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display Agentless VPN user change count for all VDOMs, given VDOM name or VDOM ID. Without argument, count for current VDOM is shown.	string	

diagnose vpn ssl usr-chg del

Del Agentless VPN user change information

```
diagnose vpn ssl usr-chg del <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Delete Agentless VPN user change information for all VDOMs, given VDOM name or VDOM ID.	string	

diagnose vpn ssl usr-chg list

List Agentless VPN user change information

```
diagnose vpn ssl usr-chg list <all|vdom-name|vfid>
```

Parameter	Description	Type	Size
<all vdom-name vfid>	Display Agentless VPN user change information for all VDOMs, given VDOM name or VDOM ID. Without argument, information for current VDOM is shown.	string	

diagnose vpn ssl web-mode-test

Enable/disable random session ID in proxy URL for testing.

```
diagnose vpn ssl web-mode-test <enable>
```

Parameter	Description	Type	Size
<enable>	Enable random session ID in proxy URL for testing. disable Disable random session ID in proxy URL for testing.	string	

diagnose vpn tunnel

IPsec tunnel.

This topic includes the following commands:

- [diagnose vpn tunnel bundle-list on page 3426](#)
- [diagnose vpn tunnel bundle-list name on page 3427](#)
- [diagnose vpn tunnel bundle-list vdom on page 3427](#)
- [diagnose vpn tunnel delinbsa on page 3427](#)
- [diagnose vpn tunnel deloutbsa on page 3427](#)
- [diagnose vpn tunnel dialup-list on page 3428](#)
- [diagnose vpn tunnel down on page 3428](#)
- [diagnose vpn tunnel fec on page 3428](#)
- [diagnose vpn tunnel flush on page 3429](#)
- [diagnose vpn tunnel key-life-time on page 3429](#)
- [diagnose vpn tunnel list on page 3429](#)
- [diagnose vpn tunnel list name on page 3429](#)
- [diagnose vpn tunnel list number on page 3429](#)
- [diagnose vpn tunnel route4-priority on page 3430](#)
- [diagnose vpn tunnel route6-priority on page 3430](#)
- [diagnose vpn tunnel stat on page 3430](#)
- [diagnose vpn tunnel stat flush on page 3430](#)
- [diagnose vpn tunnel up on page 3430](#)

diagnose vpn tunnel bundle-list

List all bundles.

```
diagnose vpn tunnel bundle-list
```

diagnose vpn tunnel bundle-list name

List bundle by interface.

```
diagnose vpn tunnel bundle-list name
```

diagnose vpn tunnel bundle-list vdom

List bundle by VDOM.

```
diagnose vpn tunnel bundle-list vdom
```

diagnose vpn tunnel delinbsa

Remove tunnel sa.

```
diagnose vpn tunnel delinbsa <name> <spi> <spi> <spi> <spi> <spi> <spi> <spi> <spi>
```

Parameter	Description	Type	Size
<name>	Name of tunnel.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	

diagnose vpn tunnel deloutbsa

Remove tunnel sa.

```
diagnose vpn tunnel deloutbsa <name> <spi> <spi> <spi> <spi> <spi> <spi> <spi> <spi>
```

Parameter	Description	Type	Size
<name>	Name of tunnel.	string	

Parameter	Description	Type	Size
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	
<spi>	SA SPI.	string	

diagnose vpn tunnel dialup-list

List dialup tunnel.

```
diagnose vpn tunnel dialup-list
```

diagnose vpn tunnel down

Shut down tunnel.

```
diagnose vpn tunnel down <phase2> <phase1> <serial>
```

Parameter	Description	Type	Size
<phase2>	Name of phase2.	string	
<phase1>	Name of phase1.	string	
<serial>	Phase2 serial number.	string	

diagnose vpn tunnel fec

FEC statistics.

```
diagnose vpn tunnel fec <phase1> <1>
```

Parameter	Description	Type	Size
<phase1>	Name of phase1.	string	
<1>	Clean the statistic.	string	

diagnose vpn tunnel flush

Flush tunnel SAs.

```
diagnose vpn tunnel flush
```

diagnose vpn tunnel key-life-time

Override configured IPsec SA lifetime with specified value.

```
diagnose vpn tunnel key-life-time <life-time>
```

Parameter	Description	Type	Size
<life-time>	Life-time in seconds.	string	

diagnose vpn tunnel list

List all tunnel.

```
diagnose vpn tunnel list
```

diagnose vpn tunnel list name

List tunnel by name.

```
diagnose vpn tunnel list name
```

diagnose vpn tunnel list number

List tunnel by number.

```
diagnose vpn tunnel list number <begin-index> <end-index>
```

Parameter	Description	Type	Size
<begin-index>	First index of tunnel.	string	
<end-index>	Last index of tunnel.	string	

diagnose vpn tunnel route4-priority

Update tunnel IPv4 route priority.

```
diagnose vpn tunnel route4-priority <name> <priority>
```

Parameter	Description	Type	Size
<name>	Name of tunnel.	string	
<priority>	Priority of IPv4 route.	string	

diagnose vpn tunnel route6-priority

Update tunnel IPv6 route priority.

```
diagnose vpn tunnel route6-priority <name> <priority>
```

Parameter	Description	Type	Size
<name>	Name of tunnel.	string	
<priority>	Priority of IPv6 route.	string	

diagnose vpn tunnel stat

Tunnel statistic info.

```
diagnose vpn tunnel stat
```

diagnose vpn tunnel stat flush

Flush tunnel stats by name.

```
diagnose vpn tunnel stat flush
```

diagnose vpn tunnel up

Activate tunnel.

```
diagnose vpn tunnel up <phase2> <phase1> <serial>
```

Parameter	Description	Type	Size
<phase2>	Name of phase2.	string	
<phase1>	Name of phase1.	string	
<serial>	Phase2 serial number.	string	

diagnose wacs

Web cache DB daemon.

This topic includes the following commands:

- [diagnose wacs clear on page 3431](#)
- [diagnose wacs restart on page 3431](#)
- [diagnose wacs stats on page 3431](#)

diagnose wacs clear

Remove all entries from the database.

```
diagnose wacs clear
```

diagnose wacs restart

Restart the daemon and reset the statistical parameters.

```
diagnose wacs restart
```

diagnose wacs stats

Show statistics.

```
diagnose wacs stats
```

diagnose wad

WAD diagnostics.

This topic includes the following commands:

- [diagnose wad access-proxy on page 3443](#)
- [diagnose wad access-proxy health-check on page 3443](#)
- [diagnose wad access-proxy health-check status on page 3443](#)
- [diagnose wad config on page 3443](#)
- [diagnose wad config auth-rule on page 3443](#)
- [diagnose wad config policy on page 3443](#)
- [diagnose wad config proxy-policy on page 3444](#)
- [diagnose wad config summary on page 3444](#)
- [diagnose wad console-log on page 3444](#)
- [diagnose wad console-log disable on page 3444](#)
- [diagnose wad console-log enable on page 3444](#)
- [diagnose wad csvc on page 3444](#)
- [diagnose wad csvc bytcache on page 3445](#)
- [diagnose wad csvc bytcache clear on page 3445](#)
- [diagnose wad csvc bytcache flush on page 3445](#)
- [diagnose wad csvc bytcache lists on page 3445](#)
- [diagnose wad csvc bytcache stats on page 3445](#)
- [diagnose wad csvc bytcache toggle on page 3446](#)
- [diagnose wad csvc bytcache toggle all on page 3446](#)
- [diagnose wad csvc bytcache toggle create on page 3446](#)
- [diagnose wad csvc bytcache toggle read on page 3446](#)
- [diagnose wad csvc memcache on page 3447](#)
- [diagnose wad csvc memcache clear on page 3447](#)
- [diagnose wad csvc memcache flush on page 3447](#)
- [diagnose wad csvc memcache lists on page 3447](#)
- [diagnose wad csvc memcache stats on page 3447](#)
- [diagnose wad csvc restart on page 3448](#)
- [diagnose wad csvc webcache on page 3448](#)
- [diagnose wad csvc webcache clear on page 3448](#)
- [diagnose wad csvc webcache flush on page 3448](#)
- [diagnose wad csvc webcache lists on page 3449](#)
- [diagnose wad csvc webcache stats on page 3449](#)
- [diagnose wad csvc webcache toggle on page 3449](#)
- [diagnose wad csvc webcache toggle abort on page 3449](#)
- [diagnose wad csvc webcache toggle add_ref on page 3449](#)
- [diagnose wad csvc webcache toggle all on page 3450](#)
- [diagnose wad csvc webcache toggle append on page 3450](#)
- [diagnose wad csvc webcache toggle create on page 3450](#)
- [diagnose wad csvc webcache toggle read on page 3450](#)
- [diagnose wad csvc webcache toggle remove on page 3451](#)
- [diagnose wad csvc webcache toggle resolve on page 3451](#)

- [diagnose wad csvc webcache toggle update on page 3451](#)
- [diagnose wad debug on page 3451](#)
- [diagnose wad debug clear on page 3451](#)
- [diagnose wad debug crash on page 3452](#)
- [diagnose wad debug crash clear on page 3452](#)
- [diagnose wad debug crash disable on page 3452](#)
- [diagnose wad debug crash enable on page 3452](#)
- [diagnose wad debug crash list on page 3452](#)
- [diagnose wad debug crash max on page 3452](#)
- [diagnose wad debug crash read on page 3453](#)
- [diagnose wad debug disable on page 3453](#)
- [diagnose wad debug disable category on page 3453](#)
- [diagnose wad debug disable category antiphish on page 3453](#)
- [diagnose wad debug disable category auth on page 3453](#)
- [diagnose wad debug disable category autotest on page 3453](#)
- [diagnose wad debug disable category bytcache on page 3454](#)
- [diagnose wad debug disable category casb on page 3454](#)
- [diagnose wad debug disable category cifs on page 3454](#)
- [diagnose wad debug disable category cmgr on page 3454](#)
- [diagnose wad debug disable category config on page 3454](#)
- [diagnose wad debug disable category csvc on page 3454](#)
- [diagnose wad debug disable category detail on page 3455](#)
- [diagnose wad debug disable category devuln on page 3455](#)
- [diagnose wad debug disable category diag on page 3455](#)
- [diagnose wad debug disable category dispatcher on page 3455](#)
- [diagnose wad debug disable category dns on page 3455](#)
- [diagnose wad debug disable category dskd on page 3455](#)
- [diagnose wad debug disable category email on page 3456](#)
- [diagnose wad debug disable category ftp on page 3456](#)
- [diagnose wad debug disable category http on page 3456](#)
- [diagnose wad debug disable category http2 on page 3456](#)
- [diagnose wad debug disable category http3 on page 3456](#)
- [diagnose wad debug disable category icap on page 3456](#)
- [diagnose wad debug disable category icbsvc on page 3457](#)
- [diagnose wad debug disable category info on page 3457](#)
- [diagnose wad debug disable category ips on page 3457](#)
- [diagnose wad debug disable category mapi on page 3457](#)
- [diagnose wad debug disable category memblk on page 3457](#)
- [diagnose wad debug disable category monitor on page 3457](#)
- [diagnose wad debug disable category packet on page 3458](#)
- [diagnose wad debug disable category policy on page 3458](#)
- [diagnose wad debug disable category policy_test on page 3458](#)
- [diagnose wad debug disable category proc on page 3458](#)

- [diagnose wad debug disable category quic on page 3458](#)
- [diagnose wad debug disable category quic_cc on page 3458](#)
- [diagnose wad debug disable category rpc on page 3459](#)
- [diagnose wad debug disable category scan on page 3459](#)
- [diagnose wad debug disable category scp on page 3459](#)
- [diagnose wad debug disable category session on page 3459](#)
- [diagnose wad debug disable category sftp on page 3459](#)
- [diagnose wad debug disable category socks on page 3459](#)
- [diagnose wad debug disable category ssh on page 3460](#)
- [diagnose wad debug disable category ssl on page 3460](#)
- [diagnose wad debug disable category stream on page 3460](#)
- [diagnose wad debug disable category svc_conn on page 3460](#)
- [diagnose wad debug disable category sys on page 3460](#)
- [diagnose wad debug disable category tfap on page 3460](#)
- [diagnose wad debug disable category tls_fingerprint on page 3461](#)
- [diagnose wad debug disable category tunnel on page 3461](#)
- [diagnose wad debug disable category uih on page 3461](#)
- [diagnose wad debug disable category video on page 3461](#)
- [diagnose wad debug disable category vs on page 3461](#)
- [diagnose wad debug disable category webcache on page 3461](#)
- [diagnose wad debug disable category ztna_portal on page 3462](#)
- [diagnose wad debug disable category ztna_rev_conn on page 3462](#)
- [diagnose wad debug display on page 3462](#)
- [diagnose wad debug display pid on page 3462](#)
- [diagnose wad debug display pid disable on page 3462](#)
- [diagnose wad debug display pid enable on page 3462](#)
- [diagnose wad debug enable on page 3463](#)
- [diagnose wad debug enable all on page 3463](#)
- [diagnose wad debug enable category on page 3463](#)
- [diagnose wad debug enable category all on page 3463](#)
- [diagnose wad debug enable category antiphish on page 3463](#)
- [diagnose wad debug enable category auth on page 3463](#)
- [diagnose wad debug enable category autotest on page 3464](#)
- [diagnose wad debug enable category bytcache on page 3464](#)
- [diagnose wad debug enable category casb on page 3464](#)
- [diagnose wad debug enable category cifs on page 3464](#)
- [diagnose wad debug enable category cmgr on page 3464](#)
- [diagnose wad debug enable category config on page 3464](#)
- [diagnose wad debug enable category csvc on page 3465](#)
- [diagnose wad debug enable category detail on page 3465](#)
- [diagnose wad debug enable category devuln on page 3465](#)
- [diagnose wad debug enable category diag on page 3465](#)
- [diagnose wad debug enable category dispatcher on page 3465](#)

- [diagnose wad debug enable category dns on page 3465](#)
- [diagnose wad debug enable category dskd on page 3466](#)
- [diagnose wad debug enable category email on page 3466](#)
- [diagnose wad debug enable category ftp on page 3466](#)
- [diagnose wad debug enable category http on page 3466](#)
- [diagnose wad debug enable category http2 on page 3466](#)
- [diagnose wad debug enable category http3 on page 3466](#)
- [diagnose wad debug enable category icap on page 3467](#)
- [diagnose wad debug enable category icbsvc on page 3467](#)
- [diagnose wad debug enable category info on page 3467](#)
- [diagnose wad debug enable category ips on page 3467](#)
- [diagnose wad debug enable category mapi on page 3467](#)
- [diagnose wad debug enable category memblk on page 3467](#)
- [diagnose wad debug enable category monitor on page 3468](#)
- [diagnose wad debug enable category packet on page 3468](#)
- [diagnose wad debug enable category policy on page 3468](#)
- [diagnose wad debug enable category policy_test on page 3468](#)
- [diagnose wad debug enable category proc on page 3468](#)
- [diagnose wad debug enable category quic on page 3468](#)
- [diagnose wad debug enable category quic_cc on page 3469](#)
- [diagnose wad debug enable category rpc on page 3469](#)
- [diagnose wad debug enable category scan on page 3469](#)
- [diagnose wad debug enable category scp on page 3469](#)
- [diagnose wad debug enable category session on page 3469](#)
- [diagnose wad debug enable category sftp on page 3469](#)
- [diagnose wad debug enable category socks on page 3470](#)
- [diagnose wad debug enable category ssh on page 3470](#)
- [diagnose wad debug enable category ssl on page 3470](#)
- [diagnose wad debug enable category stream on page 3470](#)
- [diagnose wad debug enable category svc_conn on page 3470](#)
- [diagnose wad debug enable category sys on page 3470](#)
- [diagnose wad debug enable category tfap on page 3471](#)
- [diagnose wad debug enable category tls_fingerprint on page 3471](#)
- [diagnose wad debug enable category tunnel on page 3471](#)
- [diagnose wad debug enable category uih on page 3471](#)
- [diagnose wad debug enable category video on page 3471](#)
- [diagnose wad debug enable category vs on page 3471](#)
- [diagnose wad debug enable category webcache on page 3472](#)
- [diagnose wad debug enable category ztna_portal on page 3472](#)
- [diagnose wad debug enable category ztna_rev_conn on page 3472](#)
- [diagnose wad debug enable level on page 3472](#)
- [diagnose wad debug enable level error on page 3472](#)
- [diagnose wad debug enable level info on page 3472](#)

- [diagnose wad debug enable level verbose on page 3473](#)
- [diagnose wad debug enable level warn on page 3473](#)
- [diagnose wad debug ips-db on page 3473](#)
- [diagnose wad debug ips-db status on page 3473](#)
- [diagnose wad debug ips-filter on page 3473](#)
- [diagnose wad debug ips-filter aid on page 3473](#)
- [diagnose wad debug ips-filter all on page 3474](#)
- [diagnose wad debug ips-filter clear on page 3474](#)
- [diagnose wad debug ips-filter show on page 3474](#)
- [diagnose wad debug ips-filter vid on page 3474](#)
- [diagnose wad debug save-http-req-crash on page 3474](#)
- [diagnose wad debug save-http-req-crash disable on page 3474](#)
- [diagnose wad debug save-http-req-crash enable on page 3475](#)
- [diagnose wad debug show on page 3475](#)
- [diagnose wad dev on page 3475](#)
- [diagnose wad dev fcnacd on page 3475](#)
- [diagnose wad dev fcnacd delete on page 3475](#)
- [diagnose wad dev fcnacd ip-err on page 3475](#)
- [diagnose wad dev fcnacd uid-err on page 3476](#)
- [diagnose wad dev fcnacd update on page 3476](#)
- [diagnose wad dev query-by on page 3476](#)
- [diagnose wad dev query-by ipv4 on page 3476](#)
- [diagnose wad dev query-by ipv6 on page 3476](#)
- [diagnose wad dev query-by uid on page 3476](#)
- [diagnose wad dev-vuln on page 3477](#)
- [diagnose wad dev-vuln query on page 3477](#)
- [diagnose wad dev-vuln query-by-id on page 3477](#)
- [diagnose wad dev-vuln query-ftgd on page 3477](#)
- [diagnose wad filter on page 3477](#)
- [diagnose wad filter clear on page 3477](#)
- [diagnose wad filter dport on page 3478](#)
- [diagnose wad filter drop-unknown-session on page 3478](#)
- [diagnose wad filter dst on page 3478](#)
- [diagnose wad filter dst6 on page 3478](#)
- [diagnose wad filter explicit-policy on page 3479](#)
- [diagnose wad filter firewall-policy on page 3479](#)
- [diagnose wad filter list on page 3479](#)
- [diagnose wad filter negate on page 3479](#)
- [diagnose wad filter process-id on page 3480](#)
- [diagnose wad filter process-id-by-src on page 3480](#)
- [diagnose wad filter process-type on page 3480](#)
- [diagnose wad filter protocol on page 3480](#)
- [diagnose wad filter proxy-policy-list-increment on page 3481](#)

- [diagnose wad filter sport on page 3481](#)
- [diagnose wad filter src on page 3481](#)
- [diagnose wad filter src6 on page 3482](#)
- [diagnose wad filter vd on page 3482](#)
- [diagnose wad health on page 3482](#)
- [diagnose wad health debug on page 3482](#)
- [diagnose wad health fs on page 3482](#)
- [diagnose wad health worker on page 3483](#)
- [diagnose wad history on page 3483](#)
- [diagnose wad history clear on page 3483](#)
- [diagnose wad history list on page 3483](#)
- [diagnose wad kxp on page 3483](#)
- [diagnose wad kxp clear on page 3484](#)
- [diagnose wad kxp list on page 3484](#)
- [diagnose wad memory on page 3484](#)
- [diagnose wad memory monitor on page 3484](#)
- [diagnose wad memory monitor disable on page 3484](#)
- [diagnose wad memory monitor enable on page 3484](#)
- [diagnose wad memory monitor interval on page 3485](#)
- [diagnose wad memory monitor list on page 3485](#)
- [diagnose wad memory monitor max-report-files on page 3485](#)
- [diagnose wad memory monitor mem-threshold-red on page 3485](#)
- [diagnose wad memory overused on page 3485](#)
- [diagnose wad memory report on page 3486](#)
- [diagnose wad memory sum on page 3486](#)
- [diagnose wad memory track on page 3486](#)
- [diagnose wad memory workers on page 3486](#)
- [diagnose wad process on page 3486](#)
- [diagnose wad process YouTube-filter-cache-service on page 3487](#)
- [diagnose wad process algo on page 3489](#)
- [diagnose wad process byte-cache on page 3491](#)
- [diagnose wad process cache-service-cs on page 3493](#)
- [diagnose wad process cache-service-db on page 3495](#)
- [diagnose wad process cert-inspection on page 3497](#)
- [diagnose wad process cert-manager on page 3499](#)
- [diagnose wad process config-notify on page 3501](#)
- [diagnose wad process debug on page 3503](#)
- [diagnose wad process dev-vuln on page 3505](#)
- [diagnose wad process dispatcher on page 3507](#)
- [diagnose wad process informer on page 3509](#)
- [diagnose wad process inline-ips-pktlog on page 3511](#)
- [diagnose wad process manager on page 3513](#)
- [diagnose wad process object-cache on page 3515](#)

- [diagnose wad process reverse-connector on page 3517](#)
- [diagnose wad process staled-worker on page 3519](#)
- [diagnose wad process user-info on page 3521](#)
- [diagnose wad process user-info-history on page 3523](#)
- [diagnose wad process worker on page 3525](#)
- [diagnose wad report on page 3527](#)
- [diagnose wad report policy on page 3527](#)
- [diagnose wad report session on page 3527](#)
- [diagnose wad report user on page 3527](#)
- [diagnose wad restore on page 3527](#)
- [diagnose wad restore cdn-rules on page 3527](#)
- [diagnose wad restore cdn-rules all on page 3528](#)
- [diagnose wad session on page 3528](#)
- [diagnose wad session clear on page 3528](#)
- [diagnose wad session list on page 3528](#)
- [diagnose wad session list-http2 on page 3528](#)
- [diagnose wad stats on page 3528](#)
- [diagnose wad stats algo on page 3529](#)
- [diagnose wad stats algo.antiphish on page 3529](#)
- [diagnose wad stats algo.casb on page 3529](#)
- [diagnose wad stats algo.dev_info on page 3529](#)
- [diagnose wad stats algo.dev_type on page 3529](#)
- [diagnose wad stats algo.fw_policy on page 3530](#)
- [diagnose wad stats algo.icap_client on page 3530](#)
- [diagnose wad stats algo.ips on page 3530](#)
- [diagnose wad stats algo.ips_builder on page 3530](#)
- [diagnose wad stats algo.proc_common on page 3531](#)
- [diagnose wad stats algo.sec_prof on page 3531](#)
- [diagnose wad stats algo.ssl on page 3531](#)
- [diagnose wad stats algo.url_filter on page 3531](#)
- [diagnose wad stats cache_service on page 3532](#)
- [diagnose wad stats cache_service.proc_common on page 3532](#)
- [diagnose wad stats cache_service.tcp on page 3532](#)
- [diagnose wad stats cic on page 3532](#)
- [diagnose wad stats cic.proc_common on page 3532](#)
- [diagnose wad stats cmgr on page 3533](#)
- [diagnose wad stats cmgr.cert_cache on page 3533](#)
- [diagnose wad stats cmgr.cert_service on page 3533](#)
- [diagnose wad stats cmgr.dns_req on page 3533](#)
- [diagnose wad stats cmgr.http_engine on page 3534](#)
- [diagnose wad stats cmgr.proc_common on page 3534](#)
- [diagnose wad stats cmgr.quic on page 3534](#)
- [diagnose wad stats cmgr.ssl on page 3534](#)

- [diagnose wad stats cmgr.tcp on page 3535](#)
- [diagnose wad stats common on page 3535](#)
- [diagnose wad stats common.dc_ad_dns on page 3535](#)
- [diagnose wad stats common.diag on page 3535](#)
- [diagnose wad stats common.sched on page 3535](#)
- [diagnose wad stats common.ses_stats on page 3536](#)
- [diagnose wad stats common.waps on page 3536](#)
- [diagnose wad stats config on page 3536](#)
- [diagnose wad stats config.proc_common on page 3536](#)
- [diagnose wad stats config.stream_scan on page 3537](#)
- [diagnose wad stats debug on page 3537](#)
- [diagnose wad stats debug.crash_handler on page 3537](#)
- [diagnose wad stats debug.proc_common on page 3537](#)
- [diagnose wad stats dev_vuln on page 3538](#)
- [diagnose wad stats dev_vuln.dns_req on page 3538](#)
- [diagnose wad stats dev_vuln.proc_common on page 3538](#)
- [diagnose wad stats dev_vuln.ssl on page 3538](#)
- [diagnose wad stats dev_vuln.tcp on page 3538](#)
- [diagnose wad stats dispatcher on page 3539](#)
- [diagnose wad stats dispatcher.cifs on page 3539](#)
- [diagnose wad stats dispatcher.dns_proxy on page 3539](#)
- [diagnose wad stats dispatcher.proc_common on page 3539](#)
- [diagnose wad stats dispatcher.ssh on page 3540](#)
- [diagnose wad stats dispatcher.tcp on page 3540](#)
- [diagnose wad stats dispatcher.tunnel on page 3540](#)
- [diagnose wad stats informer on page 3540](#)
- [diagnose wad stats informer.dev_info on page 3541](#)
- [diagnose wad stats informer.dev_type on page 3541](#)
- [diagnose wad stats informer.proc_common on page 3541](#)
- [diagnose wad stats informer.usr_info_common on page 3541](#)
- [diagnose wad stats informer.ztna_jwt on page 3541](#)
- [diagnose wad stats mgr on page 3542](#)
- [diagnose wad stats mgr.proc_common on page 3542](#)
- [diagnose wad stats uih on page 3542](#)
- [diagnose wad stats uih.proc_common on page 3542](#)
- [diagnose wad stats usr_info on page 3543](#)
- [diagnose wad stats usr_info.dev_info on page 3543](#)
- [diagnose wad stats usr_info.dev_type on page 3543](#)
- [diagnose wad stats usr_info.dns_req on page 3543](#)
- [diagnose wad stats usr_info.proc_common on page 3544](#)
- [diagnose wad stats usr_info.ssl on page 3544](#)
- [diagnose wad stats usr_info.tcp on page 3544](#)
- [diagnose wad stats usr_info.usr_info_common on page 3544](#)

- [diagnose wad stats vfcs on page 3544](#)
- [diagnose wad stats vfcs.proc_common on page 3545](#)
- [diagnose wad stats worker on page 3545](#)
- [diagnose wad stats worker.antiphish on page 3545](#)
- [diagnose wad stats worker.app_mgr on page 3545](#)
- [diagnose wad stats worker.casb on page 3546](#)
- [diagnose wad stats worker.casb_eng on page 3546](#)
- [diagnose wad stats worker.cert_cache on page 3546](#)
- [diagnose wad stats worker.cifs on page 3546](#)
- [diagnose wad stats worker.config_delta on page 3547](#)
- [diagnose wad stats worker.conn_pool on page 3547](#)
- [diagnose wad stats worker.dev_info on page 3547](#)
- [diagnose wad stats worker.dev_type on page 3547](#)
- [diagnose wad stats worker.digest on page 3547](#)
- [diagnose wad stats worker.dns_proxy on page 3548](#)
- [diagnose wad stats worker.dns_req on page 3548](#)
- [diagnose wad stats worker.fast_match on page 3548](#)
- [diagnose wad stats worker.fw_policy on page 3548](#)
- [diagnose wad stats worker.hauth_uid_cache on page 3549](#)
- [diagnose wad stats worker.http_engine on page 3549](#)
- [diagnose wad stats worker.http_ffbk on page 3549](#)
- [diagnose wad stats worker.http_scan on page 3549](#)
- [diagnose wad stats worker.http_srv_selector on page 3550](#)
- [diagnose wad stats worker.icap_client on page 3550](#)
- [diagnose wad stats worker.icap_parser on page 3550](#)
- [diagnose wad stats worker.icap_remote_server on page 3550](#)
- [diagnose wad stats worker.infection_cache on page 3550](#)
- [diagnose wad stats worker.ipseng on page 3551](#)
- [diagnose wad stats worker.pol_test on page 3551](#)
- [diagnose wad stats worker.policy_profile on page 3551](#)
- [diagnose wad stats worker.proc_common on page 3551](#)
- [diagnose wad stats worker.protos on page 3552](#)
- [diagnose wad stats worker.quic on page 3552](#)
- [diagnose wad stats worker.saml on page 3552](#)
- [diagnose wad stats worker.sec_prof on page 3552](#)
- [diagnose wad stats worker.ssh on page 3553](#)
- [diagnose wad stats worker.ssl on page 3553](#)
- [diagnose wad stats worker.sysmem on page 3553](#)
- [diagnose wad stats worker.tcp on page 3553](#)
- [diagnose wad stats worker.traffic_mirror on page 3553](#)
- [diagnose wad stats worker.tunnel on page 3554](#)
- [diagnose wad stats worker.url_filter on page 3554](#)
- [diagnose wad stats worker.usr_info_common on page 3554](#)

- [diagnose wad stats worker.vs_cert_cache on page 3554](#)
- [diagnose wad stats worker.ztna_jwt on page 3555](#)
- [diagnose wad stream-scan on page 3555](#)
- [diagnose wad stream-scan av-intf on page 3555](#)
- [diagnose wad stream-scan av-intf disable on page 3555](#)
- [diagnose wad stream-scan av-intf enable on page 3555](#)
- [diagnose wad stream-scan av-test on page 3556](#)
- [diagnose wad toggle on page 3556](#)
- [diagnose wad tunnel on page 3556](#)
- [diagnose wad tunnel clear on page 3556](#)
- [diagnose wad tunnel list on page 3556](#)
- [diagnose wad uih on page 3557](#)
- [diagnose wad uih chart on page 3557](#)
- [diagnose wad uih chart range on page 3557](#)
- [diagnose wad uih chart summary on page 3557](#)
- [diagnose wad user on page 3557](#)
- [diagnose wad user clear on page 3557](#)
- [diagnose wad user device on page 3558](#)
- [diagnose wad user domain-controller on page 3558](#)
- [diagnose wad user domain-controller dns on page 3558](#)
- [diagnose wad user domain-controller dns list on page 3558](#)
- [diagnose wad user domain-controller dns test on page 3558](#)
- [diagnose wad user exchange on page 3558](#)
- [diagnose wad user exchange get-matches on page 3559](#)
- [diagnose wad user exchange query-rows on page 3559](#)
- [diagnose wad user exchange reset on page 3559](#)
- [diagnose wad user exchange resolve-names on page 3559](#)
- [diagnose wad user exchange test-auto-discover on page 3559](#)
- [diagnose wad user list on page 3559](#)
- [diagnose wad webcache on page 3560](#)
- [diagnose wad webcache clear on page 3560](#)
- [diagnose wad webcache list on page 3560](#)
- [diagnose wad worker on page 3560](#)
- [diagnose wad worker async-ut on page 3560](#)
- [diagnose wad worker avscan on page 3561](#)
- [diagnose wad worker avscan clear on page 3561](#)
- [diagnose wad worker avscan list on page 3561](#)
- [diagnose wad worker bytcache on page 3561](#)
- [diagnose wad worker bytcache clear on page 3561](#)
- [diagnose wad worker bytcache flush on page 3561](#)
- [diagnose wad worker bytcache stats on page 3562](#)
- [diagnose wad worker bytcache toggle on page 3562](#)
- [diagnose wad worker bytcache toggle all on page 3562](#)

- [diagnose wad worker bytcache toggle config on page 3562](#)
- [diagnose wad worker bytcache toggle create on page 3563](#)
- [diagnose wad worker bytcache toggle read on page 3563](#)
- [diagnose wad worker cookie on page 3563](#)
- [diagnose wad worker cookie clear-cors on page 3563](#)
- [diagnose wad worker cookie list-cors on page 3563](#)
- [diagnose wad worker cookie map on page 3564](#)
- [diagnose wad worker filter on page 3564](#)
- [diagnose wad worker filter clear on page 3564](#)
- [diagnose wad worker filter list on page 3564](#)
- [diagnose wad worker memcache on page 3564](#)
- [diagnose wad worker memcache clear on page 3564](#)
- [diagnose wad worker memcache flush on page 3565](#)
- [diagnose wad worker memcache stats on page 3565](#)
- [diagnose wad worker memcache toggle on page 3565](#)
- [diagnose wad worker memcache toggle all on page 3565](#)
- [diagnose wad worker memcache toggle config on page 3565](#)
- [diagnose wad worker memcache toggle create on page 3566](#)
- [diagnose wad worker memcache toggle read on page 3566](#)
- [diagnose wad worker peer on page 3566](#)
- [diagnose wad worker peer clear on page 3566](#)
- [diagnose wad worker peer list on page 3566](#)
- [diagnose wad worker policy on page 3567](#)
- [diagnose wad worker policy clear on page 3567](#)
- [diagnose wad worker policy list on page 3567](#)
- [diagnose wad worker restart on page 3567](#)
- [diagnose wad worker saml on page 3567](#)
- [diagnose wad worker scripts on page 3568](#)
- [diagnose wad worker scripts clear on page 3568](#)
- [diagnose wad worker scripts list on page 3568](#)
- [diagnose wad worker webcache on page 3568](#)
- [diagnose wad worker webcache clear on page 3568](#)
- [diagnose wad worker webcache flush on page 3568](#)
- [diagnose wad worker webcache stats on page 3569](#)
- [diagnose wad worker webcache summary on page 3569](#)
- [diagnose wad worker webcache toggle on page 3569](#)
- [diagnose wad worker webcache toggle abort on page 3569](#)
- [diagnose wad worker webcache toggle add_ref on page 3569](#)
- [diagnose wad worker webcache toggle all on page 3570](#)
- [diagnose wad worker webcache toggle append on page 3570](#)
- [diagnose wad worker webcache toggle config on page 3570](#)
- [diagnose wad worker webcache toggle create on page 3570](#)
- [diagnose wad worker webcache toggle read on page 3571](#)

- [diagnose wad worker webcache toggle remove on page 3571](#)
- [diagnose wad worker webcache toggle resolve on page 3571](#)
- [diagnose wad worker webcache toggle update on page 3571](#)

diagnose wad access-proxy

Show connectivity status with the real server.

```
diagnose wad access-proxy
```

diagnose wad access-proxy health-check

Show connectivity status with the real server.

```
diagnose wad access-proxy health-check
```

diagnose wad access-proxy health-check status

Show connectivity status with the real server.

```
diagnose wad access-proxy health-check status
```

diagnose wad config

CMDB share memroy.

```
diagnose wad config
```

diagnose wad config auth-rule

list firewall authentication rule

```
diagnose wad config auth-rule
```

diagnose wad config policy

list firewall policy details

```
diagnose wad config policy
```

diagnose wad config proxy-policy

list firewall explicit policy details

```
diagnose wad config proxy-policy
```

diagnose wad config summary

list basic stats while building share memory

```
diagnose wad config summary
```

diagnose wad console-log

Send WAD log messages to the console.

```
diagnose wad console-log
```

diagnose wad console-log disable

Disable logging.

```
diagnose wad console-log disable
```

diagnose wad console-log enable

Enable logging.

```
diagnose wad console-log enable
```

diagnose wad csvc

Cache service diagnostics.

```
diagnose wad csvc
```

diagnose wad csvc bytecache

Bytecache diagnostics.

```
diagnose wad csvc bytecache
```

diagnose wad csvc bytecache clear

Purge all entries.

```
diagnose wad csvc bytecache clear [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc bytecache flush

Reset statistics.

```
diagnose wad csvc bytecache flush [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc bytecache lists

Show entry lists.

```
diagnose wad csvc bytecache lists [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc bytecache stats

Show statistics.

```
diagnose wad csvc bytecache stats [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc bytecache toggle

Toggle operations to storage.

```
diagnose wad csvc bytecache toggle
```

diagnose wad csvc bytecache toggle all

Set/unset all operations as busy.

```
diagnose wad csvc bytecache toggle all [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc bytecache toggle create

Toggle create as busy.

```
diagnose wad csvc bytecache toggle create [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc bytecache toggle read

Toggle read as busy.

```
diagnose wad csvc bytecache toggle read [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc memcache

Memcache diagnostics.

```
diagnose wad csvc memcache
```

diagnose wad csvc memcache clear

Purge all entries.

```
diagnose wad csvc memcache clear [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc memcache flush

Reset statistics.

```
diagnose wad csvc memcache flush [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc memcache lists

Show entry lists.

```
diagnose wad csvc memcache lists [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc memcache stats

Show statistics.

```
diagnose wad csvc memcache stats [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc restart

Restart cache service.

```
diagnose wad csvc restart [<type>] [<index>]
```

Parameter	Description	Type	Size
[<type>]	CSVC type {0:web_cache, 1:byte_and_mem_cache} or all if not set.	string	
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache

Webcache diagnostics.

```
diagnose wad csvc webcache
```

diagnose wad csvc webcache clear

Purge all entries.

```
diagnose wad csvc webcache clear [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache flush

Reset statistics.

```
diagnose wad csvc webcache flush [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache lists

Show entry lists.

```
diagnose wad csvc webcache lists [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache stats

Show statistics.

```
diagnose wad csvc webcache stats [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle

Toggle operations to storage.

```
diagnose wad csvc webcache toggle
```

diagnose wad csvc webcache toggle abort

Toggle abort as busy.

```
diagnose wad csvc webcache toggle abort [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle add_ref

Toggle add_ref as busy.

```
diagnose wad csvc webcache toggle add_ref [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle all

Set/unset all operations as busy.

```
diagnose wad csvc webcache toggle all [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle append

Toggle append as busy.

```
diagnose wad csvc webcache toggle append [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle create

Toggle create as busy.

```
diagnose wad csvc webcache toggle create [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle read

Toggle read as busy.

```
diagnose wad csvc webcache toggle read [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle remove

Toggle remove as busy.

```
diagnose wad csvc webcache toggle remove [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle resolve

Toggle resolve as busy.

```
diagnose wad csvc webcache toggle resolve [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad csvc webcache toggle update

Toggle update as busy.

```
diagnose wad csvc webcache toggle update [<index>]
```

Parameter	Description	Type	Size
[<index>]	CSVC index or all cache services if not set.	string	

diagnose wad debug

Debug setting.

```
diagnose wad debug
```

diagnose wad debug clear

Clear debug setting.

```
diagnose wad debug clear
```

diagnose wad debug crash

Saved debug message.

```
diagnose wad debug crash
```

diagnose wad debug crash clear

Clear saved debug log.

```
diagnose wad debug crash clear
```

diagnose wad debug crash disable

Disable saving debug messages when process crashes.

```
diagnose wad debug crash disable
```

diagnose wad debug crash enable

Enable saving debug messages when process crashes.

```
diagnose wad debug crash enable
```

diagnose wad debug crash list

List a summary of crash logs.

```
diagnose wad debug crash list
```

diagnose wad debug crash max

Max save size. 1-10 (MB)

```
diagnose wad debug crash max <size>
```

Parameter	Description	Type	Size
<size>	1-10 (MB).	string	

diagnose wad debug crash read

Display saved debug log.

```
diagnose wad debug crash read <proc_type> <id>
```

Parameter	Description	Type	Size
<proc_type>	Please input proc_type number.	string	
<id>	Please input crash id.	string	

diagnose wad debug disable

Disable debug setting.

```
diagnose wad debug disable
```

diagnose wad debug disable category

Category debug setting.

```
diagnose wad debug disable category
```

diagnose wad debug disable category antiphish

Anti-Phishing

```
diagnose wad debug disable category antiphish
```

diagnose wad debug disable category auth

authentication

```
diagnose wad debug disable category auth
```

diagnose wad debug disable category autotest

auto test

```
diagnose wad debug disable category autotest
```

diagnose wad debug disable category bytecache

byte cache

```
diagnose wad debug disable category bytecache
```

diagnose wad debug disable category casb

casb

```
diagnose wad debug disable category casb
```

diagnose wad debug disable category cifs

cifs

```
diagnose wad debug disable category cifs
```

diagnose wad debug disable category cmgr

certificate management

```
diagnose wad debug disable category cmgr
```

diagnose wad debug disable category config

learn config

```
diagnose wad debug disable category config
```

diagnose wad debug disable category csvc

cache service

```
diagnose wad debug disable category csvc
```

diagnose wad debug disable category detail

troubleshoot detail

```
diagnose wad debug disable category detail
```

diagnose wad debug disable category devuln

device vulnerability

```
diagnose wad debug disable category devuln
```

diagnose wad debug disable category diag

debug daemon

```
diagnose wad debug disable category diag
```

diagnose wad debug disable category dispatcher

dispatcher

```
diagnose wad debug disable category dispatcher
```

diagnose wad debug disable category dns

DNS proxy

```
diagnose wad debug disable category dns
```

diagnose wad debug disable category dskd

cache disks

```
diagnose wad debug disable category dskd
```

diagnose wad debug disable category email

user email stats

```
diagnose wad debug disable category email
```

diagnose wad debug disable category ftp

ftp

```
diagnose wad debug disable category ftp
```

diagnose wad debug disable category http

http

```
diagnose wad debug disable category http
```

diagnose wad debug disable category http2

http2

```
diagnose wad debug disable category http2
```

diagnose wad debug disable category http3

http3

```
diagnose wad debug disable category http3
```

diagnose wad debug disable category icap

icap

```
diagnose wad debug disable category icap
```


diagnose wad debug disable category icbsvc

icb service

```
diagnose wad debug disable category icbsvc
```

diagnose wad debug disable category info

user device info

```
diagnose wad debug disable category info
```

diagnose wad debug disable category ips

ips

```
diagnose wad debug disable category ips
```

diagnose wad debug disable category mapi

mapi

```
diagnose wad debug disable category mapi
```

diagnose wad debug disable category memblk

memory block

```
diagnose wad debug disable category memblk
```

diagnose wad debug disable category monitor

worker health monitor

```
diagnose wad debug disable category monitor
```

diagnose wad debug disable category packet

packet

```
diagnose wad debug disable category packet
```

diagnose wad debug disable category policy

policy matching

```
diagnose wad debug disable category policy
```

diagnose wad debug disable category policy_test

firewall policy test

```
diagnose wad debug disable category policy_test
```

diagnose wad debug disable category proc

process management

```
diagnose wad debug disable category proc
```

diagnose wad debug disable category quic

quic

```
diagnose wad debug disable category quic
```

diagnose wad debug disable category quic_cc

quic congestion control and loss detection

```
diagnose wad debug disable category quic_cc
```

diagnose wad debug disable category rpc

rpc

```
diagnose wad debug disable category rpc
```

diagnose wad debug disable category scan

UTM scan

```
diagnose wad debug disable category scan
```

diagnose wad debug disable category scp

scp

```
diagnose wad debug disable category scp
```

diagnose wad debug disable category session

session

```
diagnose wad debug disable category session
```

diagnose wad debug disable category sftp

sftp

```
diagnose wad debug disable category sftp
```

diagnose wad debug disable category socks

socks

```
diagnose wad debug disable category socks
```

diagnose wad debug disable category ssh

ssh

```
diagnose wad debug disable category ssh
```

diagnose wad debug disable category ssl

ssl

```
diagnose wad debug disable category ssl
```

diagnose wad debug disable category stream

stream

```
diagnose wad debug disable category stream
```

diagnose wad debug disable category svc_conn

ztna service connector

```
diagnose wad debug disable category svc_conn
```

diagnose wad debug disable category sys

sys

```
diagnose wad debug disable category sys
```

diagnose wad debug disable category tfap

ztna traffic forward proxy

```
diagnose wad debug disable category tfap
```

diagnose wad debug disable category tls_fingerprint

tls fingerprint

```
diagnose wad debug disable category tls_fingerprint
```

diagnose wad debug disable category tunnel

wanopt tunnel

```
diagnose wad debug disable category tunnel
```

diagnose wad debug disable category uih

uih

```
diagnose wad debug disable category uih
```

diagnose wad debug disable category video

cache video

```
diagnose wad debug disable category video
```

diagnose wad debug disable category vs

virtual server

```
diagnose wad debug disable category vs
```

diagnose wad debug disable category webcache

webcache

```
diagnose wad debug disable category webcache
```

diagnose wad debug disable category ztna_portal

ztna web portal

```
diagnose wad debug disable category ztna_portal
```

diagnose wad debug disable category ztna_rev_conn

ztna reverse connector

```
diagnose wad debug disable category ztna_rev_conn
```

diagnose wad debug display

Display setting.

```
diagnose wad debug display
```

diagnose wad debug display pid

Pid display in the trace.

```
diagnose wad debug display pid
```

diagnose wad debug display pid disable

Disable pid display.

```
diagnose wad debug display pid disable
```

diagnose wad debug display pid enable

Enable pid display.

```
diagnose wad debug display pid enable
```

diagnose wad debug enable

Enable debug setting.

```
diagnose wad debug enable
```

diagnose wad debug enable all

Enable all debug categories and set to the maximum level.

```
diagnose wad debug enable all
```

diagnose wad debug enable category

Category debug setting.

```
diagnose wad debug enable category
```

diagnose wad debug enable category all

all category

```
diagnose wad debug enable category all
```

diagnose wad debug enable category antiphish

Anti-Phishing

```
diagnose wad debug enable category antiphish
```

diagnose wad debug enable category auth

authentication

```
diagnose wad debug enable category auth
```

diagnose wad debug enable category autotest

auto test

```
diagnose wad debug enable category autotest
```

diagnose wad debug enable category bytecache

byte cache

```
diagnose wad debug enable category bytecache
```

diagnose wad debug enable category casb

casb

```
diagnose wad debug enable category casb
```

diagnose wad debug enable category cifs

cifs

```
diagnose wad debug enable category cifs
```

diagnose wad debug enable category cmgr

certificate management

```
diagnose wad debug enable category cmgr
```

diagnose wad debug enable category config

learn config

```
diagnose wad debug enable category config
```


diagnose wad debug enable category csvc

cache service

```
diagnose wad debug enable category csvc
```

diagnose wad debug enable category detail

troubleshoot detail

```
diagnose wad debug enable category detail
```

diagnose wad debug enable category devuln

device vulnerability

```
diagnose wad debug enable category devuln
```

diagnose wad debug enable category diag

debug daemon

```
diagnose wad debug enable category diag
```

diagnose wad debug enable category dispatcher

dispatcher

```
diagnose wad debug enable category dispatcher
```

diagnose wad debug enable category dns

DNS proxy

```
diagnose wad debug enable category dns
```

diagnose wad debug enable category dskd

cache disks

```
diagnose wad debug enable category dskd
```

diagnose wad debug enable category email

user email stats

```
diagnose wad debug enable category email
```

diagnose wad debug enable category ftp

ftp

```
diagnose wad debug enable category ftp
```

diagnose wad debug enable category http

http

```
diagnose wad debug enable category http
```

diagnose wad debug enable category http2

http2

```
diagnose wad debug enable category http2
```

diagnose wad debug enable category http3

http3

```
diagnose wad debug enable category http3
```

diagnose wad debug enable category icap

icap

```
diagnose wad debug enable category icap
```

diagnose wad debug enable category icbsvc

icb service

```
diagnose wad debug enable category icbsvc
```

diagnose wad debug enable category info

user device info

```
diagnose wad debug enable category info
```

diagnose wad debug enable category ips

ips

```
diagnose wad debug enable category ips
```

diagnose wad debug enable category mapi

mapi

```
diagnose wad debug enable category mapi
```

diagnose wad debug enable category memblk

memory block

```
diagnose wad debug enable category memblk
```

diagnose wad debug enable category monitor

worker health monitor

```
diagnose wad debug enable category monitor
```

diagnose wad debug enable category packet

packet

```
diagnose wad debug enable category packet
```

diagnose wad debug enable category policy

policy matching

```
diagnose wad debug enable category policy
```

diagnose wad debug enable category policy_test

firewall policy test

```
diagnose wad debug enable category policy_test
```

diagnose wad debug enable category proc

process management

```
diagnose wad debug enable category proc
```

diagnose wad debug enable category quic

quic

```
diagnose wad debug enable category quic
```

diagnose wad debug enable category quic_cc

quic congestion control and loss detection

```
diagnose wad debug enable category quic_cc
```

diagnose wad debug enable category rpc

rpc

```
diagnose wad debug enable category rpc
```

diagnose wad debug enable category scan

UTM scan

```
diagnose wad debug enable category scan
```

diagnose wad debug enable category scp

scp

```
diagnose wad debug enable category scp
```

diagnose wad debug enable category session

session

```
diagnose wad debug enable category session
```

diagnose wad debug enable category sftp

sftp

```
diagnose wad debug enable category sftp
```

diagnose wad debug enable category socks

socks

```
diagnose wad debug enable category socks
```

diagnose wad debug enable category ssh

ssh

```
diagnose wad debug enable category ssh
```

diagnose wad debug enable category ssl

ssl

```
diagnose wad debug enable category ssl
```

diagnose wad debug enable category stream

stream

```
diagnose wad debug enable category stream
```

diagnose wad debug enable category svc_conn

ztna service connector

```
diagnose wad debug enable category svc_conn
```

diagnose wad debug enable category sys

sys

```
diagnose wad debug enable category sys
```

diagnose wad debug enable category tfap

ztna traffic forward proxy

```
diagnose wad debug enable category tfap
```

diagnose wad debug enable category tls_fingerprint

tls fingerprint

```
diagnose wad debug enable category tls_fingerprint
```

diagnose wad debug enable category tunnel

wanopt tunnel

```
diagnose wad debug enable category tunnel
```

diagnose wad debug enable category uih

uih

```
diagnose wad debug enable category uih
```

diagnose wad debug enable category video

cache video

```
diagnose wad debug enable category video
```

diagnose wad debug enable category vs

virtual server

```
diagnose wad debug enable category vs
```

diagnose wad debug enable category webcache

webcache

```
diagnose wad debug enable category webcache
```

diagnose wad debug enable category ztna_portal

ztna web portal

```
diagnose wad debug enable category ztna_portal
```

diagnose wad debug enable category ztna_rev_conn

ztna reverse connector

```
diagnose wad debug enable category ztna_rev_conn
```

diagnose wad debug enable level

Level debug setting.

```
diagnose wad debug enable level
```

diagnose wad debug enable level error

error

```
diagnose wad debug enable level error
```

diagnose wad debug enable level info

information

```
diagnose wad debug enable level info
```


diagnose wad debug enable level verbose

verbose

```
diagnose wad debug enable level verbose
```

diagnose wad debug enable level warn

warning

```
diagnose wad debug enable level warn
```

diagnose wad debug ips-db

Inline-IPS database.

```
diagnose wad debug ips-db
```

diagnose wad debug ips-db status

Inline-IPS database status.

```
diagnose wad debug ips-db status
```

diagnose wad debug ips-filter

Inline IPS debug filter setting.

```
diagnose wad debug ips-filter
```

diagnose wad debug ips-filter aid

Enable debug for a list of attack IDs.

```
diagnose wad debug ips-filter aid <id,id,...>
```

Parameter	Description	Type	Size
<id,id,...>	Attack IDs	string	

diagnose wad debug ips-filter all

Enable debug filter for all rules

```
diagnose wad debug ips-filter all
```

diagnose wad debug ips-filter clear

Clear debug filter

```
diagnose wad debug ips-filter clear
```

diagnose wad debug ips-filter show

Show current debug filter

```
diagnose wad debug ips-filter show
```

diagnose wad debug ips-filter vid

Enable debug for a list of vulnerability IDs.

```
diagnose wad debug ips-filter vid <id,id,...>
```

Parameter	Description	Type	Size
<id,id,...>	Vulnerability IDs	string	

diagnose wad debug save-http-req-crash

Save HTTP request when WAD worker crashes.

```
diagnose wad debug save-http-req-crash
```

diagnose wad debug save-http-req-crash disable

Disable saving HTTP request when WAD worker crashes.

```
diagnose wad debug save-http-req-crash disable
```

diagnose wad debug save-http-req-crash enable

Enable saving HTTP request when WAD worker crashes.

```
diagnose wad debug save-http-req-crash enable
```

diagnose wad debug show

Show debug setting.

```
diagnose wad debug show
```

diagnose wad dev

Dev. diagnostics.

```
diagnose wad dev
```

diagnose wad dev fcnacd

Emulate fcnacd messages.

```
diagnose wad dev fcnacd
```

diagnose wad dev fcnacd delete

Delete a device by uid, sn, and tenant id. (EC_LLS_ZTNA_CMD_DEV_DELETE)

```
diagnose wad dev fcnacd delete
```

diagnose wad dev fcnacd ip-err

Generate an EMS IP address error response. (EC_LLS_ZTNA_CMD_FIND_BY_IPVD_ER_CODE)

```
diagnose wad dev fcnacd ip-err
```

diagnose wad dev fcnacd uid-err

Generate an EMS UID error response. (EC_LLS_ZTNA_CMD_FIND_BY_UID)

```
diagnose wad dev fcnacd uid-err
```

diagnose wad dev fcnacd update

Insert a dummy device. (EC_LLS_ZTNA_CMD_DEV_UPDATE)

```
diagnose wad dev fcnacd update
```

diagnose wad dev query-by

Query a device.

```
diagnose wad dev query-by
```

diagnose wad dev query-by ipv4

Query by IPv4 address.

```
diagnose wad dev query-by ipv4
```

diagnose wad dev query-by ipv6

Query by IPv6 address.

```
diagnose wad dev query-by ipv6
```

diagnose wad dev query-by uid

Query by UID.

```
diagnose wad dev query-by uid
```

diagnose wad dev-vuln

Device vulnerability diagnostics.

```
diagnose wad dev-vuln
```

diagnose wad dev-vuln query

Query dev-vuln by vendor=<xxx>&version=<xxx>&product=<xxx>&model=<xxx>

```
diagnose wad dev-vuln query
```

diagnose wad dev-vuln query-by-id

Query dev-vuln by vulnerability id=<xxx>.

```
diagnose wad dev-vuln query-by-id
```

diagnose wad dev-vuln query-ftgd

Query dev-vuln by vendor=<xxx>&version=<xxx>&product=<xxx>&model=<xxx>

```
diagnose wad dev-vuln query-ftgd
```

diagnose wad filter

Filter for listing sessions or tunnels.

```
diagnose wad filter
```

diagnose wad filter clear

Erase current filter settings.

```
diagnose wad filter clear
```

diagnose wad filter dport

Destination port range to filter by.

```
diagnose wad filter dport <port> <port>
```

Parameter	Description	Type	Size
<port>	Destination port (from).	string	
<port>	Destination port (to).	string	

diagnose wad filter drop-unknown-session

Enable drop message unknown sessions.

```
diagnose wad filter drop-unknown-session <Drop unknown sessions>
```

Parameter	Description	Type	Size
<Drop unknown sessions>	(1 = enable, 0 = do not drop).	string	

diagnose wad filter dst

Destination address range to filter by.

```
diagnose wad filter dst <ip-address> <ip-address>
```

Parameter	Description	Type	Size
<ip-address>	Destination IP address (from).	string	
<ip-address>	Destination IP address (to).	string	

diagnose wad filter dst6

Destination address6 range to filter by.

```
diagnose wad filter dst6 <ip-address6> <ip-address6>
```

Parameter	Description	Type	Size
<ip-address6>	Destination IPv6 address (from).	string	
<ip-address6>	Destination IPv6 address (to).	string	

diagnose wad filter explicit-policy

Index of explicit-policy. -1 matches all.

```
diagnose wad filter explicit-policy <index>
```

Parameter	Description	Type	Size
<index>	Index of explicit-policy. -1 matches all.	string	

diagnose wad filter firewall-policy

Index of firewall-policy. -1 matches all.

```
diagnose wad filter firewall-policy <index>
```

Parameter	Description	Type	Size
<index>	Index of firewall-policy. -1 matches all.	string	

diagnose wad filter list

Display current filter.

```
diagnose wad filter list
```

diagnose wad filter negate

Negate the specified filter parameter.

```
diagnose wad filter negate <parm>
```

Parameter	Description	Type	Size
<parm>	Filter parameter to negate.	string	

diagnose wad filter process-id

Select process ID to filter by.

```
diagnose wad filter process-id <Process ID>
```

Parameter	Description	Type	Size
<Process ID>	Process ID to filter (0 = disable).	string	

diagnose wad filter process-id-by-src

Process id affined with the selected source IPv4/IPv6 to filter by.

```
diagnose wad filter process-id-by-src <ip-address>
```

Parameter	Description	Type	Size
<ip-address>	Source IPv4/IPv6.	string	

diagnose wad filter process-type

Select process type to filter by.

```
diagnose wad filter process-type <Process types (0 = disable):>
```

Parameter	Description	Type	Size
<Process types (0 = disable):>	1. manager 2. dispatcher 3. worker 4. algo 5. informer 6. user-info 7. cache-service-cs 8. cache-service-db 9. cert-inspection 10. youtube-filter-cache-service 11. user-info-history 12. debug 13. config-notify 14. object-cache 15. byte-cache 16. traffic aggregator 17. preload daemon	string	

diagnose wad filter protocol

Select protocols to filter by.

```
diagnose wad filter protocol <http> <mapi> <cifs> <ftp> <tcp>
```

Parameter	Description	Type	Size
<http>	To match (1), otherwise (0).	string	

Parameter	Description	Type	Size
<mapi>	To match (1), otherwise (0).	string	
<cifs>	To match (1), otherwise (0).	string	
<ftp>	To match (1), otherwise (0).	string	
<tcp>	To match (1), otherwise (0).	string	

diagnose wad filter proxy-policy-list-increment

Increment in steps per proxy policy list call.

```
diagnose wad filter proxy-policy-list-increment <increment steps>
```

Parameter	Description	Type	Size
<increment steps>	Incremental steps per proxy policy call (10 - 100, default = 20)	string	

diagnose wad filter sport

Source port range to filter by.

```
diagnose wad filter sport <port> <port>
```

Parameter	Description	Type	Size
<port>	Source port (from).	string	
<port>	Source port (to).	string	

diagnose wad filter src

Source address range to filter by.

```
diagnose wad filter src <ip-address> <ip-address>
```

Parameter	Description	Type	Size
<ip-address>	Source IP address (from).	string	
<ip-address>	Source IP address (to).	string	

diagnose wad filter src6

Source address6 range to filter by.

```
diagnose wad filter src6 <ip-address6> <ip-address6>
```

Parameter	Description	Type	Size
<ip-address6>	Source IPv6 address (from).	string	
<ip-address6>	Source IPv6 address (to).	string	

diagnose wad filter vd

Virtual Domain Name.

```
diagnose wad filter vd <vdom>
```

Parameter	Description	Type	Size
<vdom>	Virtual Domain Name. ALL all vdoms	string	

diagnose wad health

Check WAD processes status for handling diagnose commands and file system health.

```
diagnose wad health
```

diagnose wad health debug

Check WAD debug daemon status for handling dianose commands.

```
diagnose wad health debug
```

diagnose wad health fs

Check file system health.

```
diagnose wad health fs <File system type (0 = all):> <Lines>
```

Parameter	Description	Type	Size
<File system type (0 = all):>	1. data file system 2. data2 file system 3. log file system	string	
<Lines>	Max write lines (1-50)	string	

diagnose wad health worker

Check WAD worker processes status for handling diagnose commands.

```
diagnose wad health worker
```

diagnose wad history

Statistics history.

```
diagnose wad history
```

diagnose wad history clear

Clear statistics history.

```
diagnose wad history clear
```

diagnose wad history list

List statistics history.

```
diagnose wad history list <proto> <period>
```

Parameter	Description	Type	Size
<proto>	All HTTP FTP CIFS MAPI TCP.	string	
<period>	10min hour day 30days.	string	

diagnose wad kxp

SSL KXP diagnostics.

```
diagnose wad kxp
```

diagnose wad kxp clear

Clear all KXP queue stats.

```
diagnose wad kxp clear
```

diagnose wad kxp list

List KXP queue size.

```
diagnose wad kxp list
```

diagnose wad memory

WAD memory diagnostics.

```
diagnose wad memory
```

diagnose wad memory monitor

Monitor wad memory usage.

```
diagnose wad memory monitor
```

diagnose wad memory monitor disable

Disable wad memory monitor.

```
diagnose wad memory monitor disable
```

diagnose wad memory monitor enable

Enable wad memory monitor.

```
diagnose wad memory monitor enable
```

diagnose wad memory monitor interval

Set the time interval (in min) for memory monitoring.

```
diagnose wad memory monitor interval <Integer>
```

Parameter	Description	Type	Size
<Integer>	Please enter an integer from <5> to <60>.	string	

diagnose wad memory monitor list

List wad memory monitor parameters.

```
diagnose wad memory monitor list
```

diagnose wad memory monitor max-report-files

Max number of report files to save.

```
diagnose wad memory monitor max-report-files <Integer>
```

Parameter	Description	Type	Size
<Integer>	Please enter an integer from <1> to <10>.	string	

diagnose wad memory monitor mem-threshold-red

Set threshold at which wad workers' total memory usage triggers saving memory report in a disk file.

```
diagnose wad memory monitor mem-threshold-red <Integer>
```

Parameter	Description	Type	Size
<Integer>	Please enter an integer from <0> to <100>.	string	

diagnose wad memory overused

List suspiciously overused WAD memory buckets.

```
diagnose wad memory overused <Integer>
```

Parameter	Description	Type	Size
<Integer>	Overused threshold filter value.	string	

diagnose wad memory report

List a report of wad memory usage.

```
diagnose wad memory report
```

diagnose wad memory sum

Sum all WAD process memory modules stats.

```
diagnose wad memory sum
```

diagnose wad memory track

Track cmem alloc.

```
diagnose wad memory track <Integer>
```

Parameter	Description	Type	Size
<Integer>	Id for cmem stats.	string	

diagnose wad memory workers

List WAD worker memory modules.

```
diagnose wad memory workers
```

diagnose wad process

Wad process diagnostics.

```
diagnose wad process
```

diagnose wad process YouTube-filter-cache-service

Diagnose YouTube-filter-cache-service process.

```
diagnose wad process YouTube-filter-cache-service <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process algo

Diagnose algo process.

```
diagnose wad process algo <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process byte-cache

Diagnose byte-cache process.

```
diagnose wad process byte-cache <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process cache-service-cs

Diagnose cache-service-cs process.

```
diagnose wad process cache-service-cs <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process cache-service-db

Diagnose cache-service-db process.

```
diagnose wad process cache-service-db <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process cert-inspection

Diagnose cert-inspection process.

```
diagnose wad process cert-inspection <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process cert-manager

Diagnose cert-manager process.

```
diagnose wad process cert-manager <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process config-notify

Diagnose config-notify process.

```
diagnose wad process config-notify <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process debug

Diagnose debug process.

```
diagnose wad process debug <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process dev-vuln

Diagnose dev-vuln process.

```
diagnose wad process dev-vuln <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process dispatcher

Diagnose dispatcher process.

```
diagnose wad process dispatcher <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process informer

Diagnose informer process.

```
diagnose wad process informer <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process inline-ips-pktlog

Diagnose inline-ips-pktlog process.

```
diagnose wad process inline-ips-pktlog <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process manager

Diagnose manager process.

```
diagnose wad process manager <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process object-cache

Diagnose object-cache process.

```
diagnose wad process object-cache <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process reverse-connector

Diagnose reverse-connector process.

```
diagnose wad process reverse-connector <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process staled-worker

Diagnose staled-worker process.

```
diagnose wad process staled-worker <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process user-info

Diagnose user-info process.

```
diagnose wad process user-info <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process user-info-history

Diagnose user-info-history process.

```
diagnose wad process user-info-history <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad process worker

Diagnose worker process.

```
diagnose wad process worker <index> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
<cmd> <cmd> <cmd> <cmd> <cmd> <cmd>
```

Parameter	Description	Type	Size
<index>	Process index to send command to. (0 for the 1st process; -1 for all)	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

Parameter	Description	Type	Size
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	
<cmd>	Diagnostic command (0 for help). Support up to 32 commands.	string	

diagnose wad report

A consolidated report and shorthand access to various 'diag test app xxx' commands.

```
diagnose wad report
```

diagnose wad report policy

Wad policy related diagnostics.

```
diagnose wad report policy
```

diagnose wad report session

Wad TCP, HTTP, and FTP session related diagnostics.

```
diagnose wad report session
```

diagnose wad report user

Wad user and auth related diagnostics.

```
diagnose wad report user
```

diagnose wad restore

Restore configuration defaults.

```
diagnose wad restore
```

diagnose wad restore cdn-rules

Restore default cdn rules.

```
diagnose wad restore cdn-rules
```

diagnose wad restore cdn-rules all

Restore default cdn rules.

```
diagnose wad restore cdn-rules all
```

diagnose wad session

Session diagnostics.

```
diagnose wad session
```

diagnose wad session clear

Clear all active sessions.

```
diagnose wad session clear
```

diagnose wad session list

List active sessions.

```
diagnose wad session list
```

diagnose wad session list-http2

List active http2 sessions.

```
diagnose wad session list-http2
```

diagnose wad stats

Statistics.

```
diagnose wad stats <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo

Show proc_algo statistics.

```
diagnose wad stats algo <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.antiphish

Show antiphish statistics.

```
diagnose wad stats algo.antiphish <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.casb

Show casb statistics.

```
diagnose wad stats algo.casb <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.dev_info

Show dev_info statistics.

```
diagnose wad stats algo.dev_info <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.dev_type

Show dev_stats statistics.

```
diagnose wad stats algo.dev_type <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.fw_policy

Show fw_policy statistics.

```
diagnose wad stats algo.fw_policy <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.icap_client

Show icap_client statistics.

```
diagnose wad stats algo.icap_client <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.ips

Show ipsscan statistics.

```
diagnose wad stats algo.ips <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.ips_builder

Show ips_builder statistics.

```
diagnose wad stats algo.ips_builder <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.proc_common

Show proc_common statistics.

```
diagnose wad stats algo.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.sec_prof

Show sec_prof statistics.

```
diagnose wad stats algo.sec_prof <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.ssl

Show ssl statistics.

```
diagnose wad stats algo.ssl <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats algo.url_filter

Show url_filter statistics.

```
diagnose wad stats algo.url_filter <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cache_service

Show proc_cache_service statistics.

```
diagnose wad stats cache_service <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cache_service.proc_common

Show proc_common statistics.

```
diagnose wad stats cache_service.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cache_service.tcp

Show tcp statistics.

```
diagnose wad stats cache_service.tcp <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cic

Show proc_cic statistics.

```
diagnose wad stats cic <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cic.proc_common

Show proc_common statistics.

```
diagnose wad stats cic.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr

Show proc_cmgr statistics.

```
diagnose wad stats cmgr <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr.cert_cache

Show cert_cache statistics.

```
diagnose wad stats cmgr.cert_cache <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr.cert_service

Show cert_service statistics.

```
diagnose wad stats cmgr.cert_service <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr.dns_req

Show dns_req statistics.

```
diagnose wad stats cmgr.dns_req <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr.http_engine

Show http_engine statistics.

```
diagnose wad stats cmgr.http_engine <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr.proc_common

Show proc_common statistics.

```
diagnose wad stats cmgr.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr.quic

Show quic statistics.

```
diagnose wad stats cmgr.quic <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr.ssl

Show ssl statistics.

```
diagnose wad stats cmgr.ssl <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats cmgr.tcp

Show tcp statistics.

```
diagnose wad stats cmgr.tcp <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats common

Show proc statistics.

```
diagnose wad stats common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats common.dc_ad_dns

Show dc_ad_dns statistics.

```
diagnose wad stats common.dc_ad_dns <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats common.diag

Show diag statistics.

```
diagnose wad stats common.diag <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats common.sched

Show sched statistics.

```
diagnose wad stats common.sched <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats common.ses_stats

Show session statistics.

```
diagnose wad stats common.ses_stats <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats common.waps

Show waps statistics.

```
diagnose wad stats common.waps <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats config

Show proc_config statistics.

```
diagnose wad stats config <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats config.proc_common

Show proc_common statistics.

```
diagnose wad stats config.proc_common <action>
```


Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats config.stream_scan

Show sscan statistics.

```
diagnose wad stats config.stream_scan <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats debug

Show proc_debug statistics.

```
diagnose wad stats debug <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats debug.crash_handler

Show crash_handler statistics.

```
diagnose wad stats debug.crash_handler <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats debug.proc_common

Show proc_common statistics.

```
diagnose wad stats debug.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dev_vuln

Show proc_dev_vuln statistics.

```
diagnose wad stats dev_vuln <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dev_vuln.dns_req

Show dns_req statistics.

```
diagnose wad stats dev_vuln.dns_req <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dev_vuln.proc_common

Show proc_common statistics.

```
diagnose wad stats dev_vuln.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dev_vuln.ssl

Show ssl statistics.

```
diagnose wad stats dev_vuln.ssl <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dev_vuln.tcp

Show tcp statistics.

```
diagnose wad stats dev_vuln.tcp <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dispatcher

Show proc_dispatcher statistics.

```
diagnose wad stats dispatcher <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dispatcher.cifs

Show cifs statistics.

```
diagnose wad stats dispatcher.cifs <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dispatcher.dns_proxy

Show dns_proxy statistics.

```
diagnose wad stats dispatcher.dns_proxy <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dispatcher.proc_common

Show proc_common statistics.

```
diagnose wad stats dispatcher.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dispatcher.ssh

Show ssh statistics.

```
diagnose wad stats dispatcher.ssh <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dispatcher.tcp

Show tcp statistics.

```
diagnose wad stats dispatcher.tcp <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats dispatcher.tunnel

Show tunnel statistics.

```
diagnose wad stats dispatcher.tunnel <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats informer

Show proc_informer statistics.

```
diagnose wad stats informer <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats informer.dev_info

Show dev_info statistics.

```
diagnose wad stats informer.dev_info <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats informer.dev_type

Show dev_stats statistics.

```
diagnose wad stats informer.dev_type <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats informer.proc_common

Show proc_common statistics.

```
diagnose wad stats informer.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats informer.usr_info_common

Show usr_info_common statistics.

```
diagnose wad stats informer.usr_info_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats informer.ztna_jwt

Show ztna_jwt statistics.

```
diagnose wad stats informer.ztna_jwt <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats mgr

Show proc_mgr statistics.

```
diagnose wad stats mgr <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats mgr.proc_common

Show proc_common statistics.

```
diagnose wad stats mgr.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats uih

Show proc_uih statistics.

```
diagnose wad stats uih <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats uih.proc_common

Show proc_common statistics.

```
diagnose wad stats uih.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats usr_info

Show proc_usr_info statistics.

```
diagnose wad stats usr_info <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats usr_info.dev_info

Show dev_info statistics.

```
diagnose wad stats usr_info.dev_info <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats usr_info.dev_type

Show dev_stats statistics.

```
diagnose wad stats usr_info.dev_type <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats usr_info.dns_req

Show dns_req statistics.

```
diagnose wad stats usr_info.dns_req <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats usr_info.proc_common

Show proc_common statistics.

```
diagnose wad stats usr_info.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats usr_info.ssl

Show ssl statistics.

```
diagnose wad stats usr_info.ssl <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats usr_info.tcp

Show tcp statistics.

```
diagnose wad stats usr_info.tcp <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats usr_info.usr_info_common

Show usr_info_common statistics.

```
diagnose wad stats usr_info.usr_info_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats vfcs

Show proc_vfcs statistics.


```
diagnose wad stats vfcs <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats vfcs.proc_common

Show proc_common statistics.

```
diagnose wad stats vfcs.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker

Show proc_worker statistics.

```
diagnose wad stats worker <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.antiphish

Show antiphish statistics.

```
diagnose wad stats worker.antiphish <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.app_mgr

Show app_mgr statistics.

```
diagnose wad stats worker.app_mgr <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.casb

Show casb statistics.

```
diagnose wad stats worker.casb <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.casb_eng

Show casb_eng statistics.

```
diagnose wad stats worker.casb_eng <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.cert_cache

Show cert_cache statistics.

```
diagnose wad stats worker.cert_cache <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.cifs

Show cifs statistics.

```
diagnose wad stats worker.cifs <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.config_delta

Show config_delta statistics.

```
diagnose wad stats worker.config_delta <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.conn_pool

Show conn_pool statistics.

```
diagnose wad stats worker.conn_pool <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.dev_info

Show dev_info statistics.

```
diagnose wad stats worker.dev_info <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.dev_type

Show dev_stats statistics.

```
diagnose wad stats worker.dev_type <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.digest

Show digest statistics.

```
diagnose wad stats worker.digest <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.dns_proxy

Show dns_proxy statistics.

```
diagnose wad stats worker.dns_proxy <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.dns_req

Show dns_req statistics.

```
diagnose wad stats worker.dns_req <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.fast_match

Show fast_match statistics.

```
diagnose wad stats worker.fast_match <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.fw_policy

Show fw_policy statistics.

```
diagnose wad stats worker.fw_policy <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.hauth_uid_cache

Show hash_cache statistics.

```
diagnose wad stats worker.hauth_uid_cache <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.http_engine

Show http_engine statistics.

```
diagnose wad stats worker.http_engine <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.http_ffbk

Show http_ffbk statistics.

```
diagnose wad stats worker.http_ffbk <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.http_scan

Show http_scan statistics.

```
diagnose wad stats worker.http_scan <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.http_srv_selector

Show http_srv_selector statistics.

```
diagnose wad stats worker.http_srv_selector <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.icap_client

Show icap_client statistics.

```
diagnose wad stats worker.icap_client <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.icap_parser

Show icap_parser statistics.

```
diagnose wad stats worker.icap_parser <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.icap_remote_server

Show icap_remote_server statistics.

```
diagnose wad stats worker.icap_remote_server <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.infection_cache

Show infection_cache statistics.

```
diagnose wad stats worker.infection_cache <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.ipseng

Show ipseng statistics.

```
diagnose wad stats worker.ipseng <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.pol_test

Show pol_test statistics.

```
diagnose wad stats worker.pol_test <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.policy_profile

Show policy_profile statistics.

```
diagnose wad stats worker.policy_profile <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.proc_common

Show proc_common statistics.

```
diagnose wad stats worker.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.protos

Show protos statistics.

```
diagnose wad stats worker.protos <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.quic

Show quic statistics.

```
diagnose wad stats worker.quic <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.saml

Show saml statistics.

```
diagnose wad stats worker.saml <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.sec_prof

Show sec_prof statistics.

```
diagnose wad stats worker.sec_prof <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.ssh

Show ssh statistics.

```
diagnose wad stats worker.ssh <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.ssl

Show ssl statistics.

```
diagnose wad stats worker.ssl <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.systemem

Show systemem statistics.

```
diagnose wad stats worker.systemem <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.tcp

Show tcp statistics.

```
diagnose wad stats worker.tcp <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.traffic_mirror

Show traffic_mirror statistics.

```
diagnose wad stats worker.traffic_mirror <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.tunnel

Show tunnel statistics.

```
diagnose wad stats worker.tunnel <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.url_filter

Show url_filter statistics.

```
diagnose wad stats worker.url_filter <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.usr_info_common

Show usr_info_common statistics.

```
diagnose wad stats worker.usr_info_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.vs_cert_cache

Show hash_cache statistics.

```
diagnose wad stats worker.vs_cert_cache <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.ztna_jwt

Show ztna_jwt statistics.

```
diagnose wad stats worker.ztna_jwt <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stream-scan

Stream scan diagnostics.

```
diagnose wad stream-scan
```

diagnose wad stream-scan av-intf

Enable/disable AV interface.

```
diagnose wad stream-scan av-intf
```

diagnose wad stream-scan av-intf disable

Disable stream scan AV interface and restart workers.

```
diagnose wad stream-scan av-intf disable
```

diagnose wad stream-scan av-intf enable

Enable stream scan AV interface and restart workers.

```
diagnose wad stream-scan av-intf enable
```

diagnose wad stream-scan av-test

AV Engine diagnostics.

```
diagnose wad stream-scan av-test <command> <worker-id>
```

Parameter	Description	Type	Size
<command>	Command to pass into AV engine. Please double quote the command.	string	
<worker-id>	Optional worker index.	string	

diagnose wad toggle

Toggle diagnose method(direct/debug proc).

```
diagnose wad toggle
```

diagnose wad tunnel

Tunnel diagnostics.

```
diagnose wad tunnel
```

diagnose wad tunnel clear

Clear all active tunnels.

```
diagnose wad tunnel clear
```

diagnose wad tunnel list

List active tunnels.

```
diagnose wad tunnel list <id>
```

Parameter	Description	Type	Size
<id>	Optional tunnel ID.	string	

diagnose wad uih

User info history diagnostics.

```
diagnose wad uih
```

diagnose wad uih chart

Display summary or range of entries of Chart DB.

```
diagnose wad uih chart
```

diagnose wad uih chart range

Display chart DB entries for <vdom> from <start> to <end>.

```
diagnose wad uih chart range
```

diagnose wad uih chart summary

Display summary of Chart DB for <vdom>.

```
diagnose wad uih chart summary
```

diagnose wad user

User diagnostics.

```
diagnose wad user
```

diagnose wad user clear

Clear all users or clear a particular user using: `diagnose wad user clear <ID> <IP|IPv6> <VDM>`.

```
diagnose wad user clear <ID> <IP> <VDM>
```

Parameter	Description	Type	Size
<ID>	Please input user ID.	string	

Parameter	Description	Type	Size
<IP>	Please input user IP.	string	
<VDOM>	Please input VDOM name the user belongs to.	string	

diagnose wad user device

Get device info.

```
diagnose wad user device
```

diagnose wad user domain-controller

Test connectivity with domain-controller.

```
diagnose wad user domain-controller
```

diagnose wad user domain-controller dns

Test DNS resolve function.

```
diagnose wad user domain-controller dns
```

diagnose wad user domain-controller dns list

Show DNS discover status on all configured user domain-controller.

```
diagnose wad user domain-controller dns list
```

diagnose wad user domain-controller dns test

Test if DNS discover function works for all configured user domain-controller.

```
diagnose wad user domain-controller dns test
```

diagnose wad user exchange

Test connectivity with user-exchange.

```
diagnose wad user exchange
```

diagnose wad user exchange get-matches

Test exact match search for Administrator.

```
diagnose wad user exchange get-matches
```

diagnose wad user exchange query-rows

Show address-book database up to 50 entries.

```
diagnose wad user exchange query-rows
```

diagnose wad user exchange reset

Close all connections related to user-exchange.

```
diagnose wad user exchange reset
```

diagnose wad user exchange resolve-names

Test pattern match search for Administrator.

```
diagnose wad user exchange resolve-names
```

diagnose wad user exchange test-auto-discover

Test if automatic discovery can work on all configured user-exchanges.

```
diagnose wad user exchange test-auto-discover
```

diagnose wad user list

List proxy users.

```
diagnose wad user list [verbose]
```

Parameter	Description	Type	Size
[verbose]	Verbose mode.	string	

diagnose wad webcache

Web cache statistics.

```
diagnose wad webcache
```

diagnose wad webcache clear

Clear web cache statistics.

```
diagnose wad webcache clear
```

diagnose wad webcache list

List web cache statistics.

```
diagnose wad webcache list <period>
```

Parameter	Description	Type	Size
<period>	10min hour day 30days.	string	

diagnose wad worker

Worker diagnostics.

```
diagnose wad worker
```

diagnose wad worker async-ut

Async Unit Test.

```
diagnose wad worker async-ut [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker avscan

Scan results statistics.

```
diagnose wad worker avscan
```

diagnose wad worker avscan clear

Clear scan results statistics.

```
diagnose wad worker avscan clear
```

diagnose wad worker avscan list

List scan results statistics.

```
diagnose wad worker avscan list
```

diagnose wad worker bytcache

Bytecache diagnostics.

```
diagnose wad worker bytcache
```

diagnose wad worker bytcache clear

Purge all entries.

```
diagnose wad worker bytcache clear [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker bytcache flush

Reset statistics.

```
diagnose wad worker bytcache flush [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker bytecache stats

Show statistics.

```
diagnose wad worker bytecache stats [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker bytecache toggle

Toggle operations.

```
diagnose wad worker bytecache toggle
```

diagnose wad worker bytecache toggle all

Set/unset all operations as busy.

```
diagnose wad worker bytecache toggle all [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker bytecache toggle config

Toggle worker bytecache config.

```
diagnose wad worker bytecache toggle config [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker bytcache toggle create

Toggle create as busy.

```
diagnose wad worker bytcache toggle create [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker bytcache toggle read

Toggle read as busy.

```
diagnose wad worker bytcache toggle read [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker cookie

Cookie information.

```
diagnose wad worker cookie
```

diagnose wad worker cookie clear-cors

Clear cookie cors info.

```
diagnose wad worker cookie clear-cors
```

diagnose wad worker cookie list-cors

Show cookie cors info.

```
diagnose wad worker cookie list-cors
```

diagnose wad worker cookie map

Show cookie map info.

```
diagnose wad worker cookie map
```

diagnose wad worker filter

Show filter statistics.

```
diagnose wad worker filter
```

diagnose wad worker filter clear

Clear filter statistics.

```
diagnose wad worker filter clear
```

diagnose wad worker filter list

List filter statistics.

```
diagnose wad worker filter list
```

diagnose wad worker memcache

Memcache diagnostics.

```
diagnose wad worker memcache
```

diagnose wad worker memcache clear

Purge all entries.

```
diagnose wad worker memcache clear [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker memcache flush

Reset statistics.

```
diagnose wad worker memcache flush [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker memcache stats

Show statistics.

```
diagnose wad worker memcache stats [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker memcache toggle

Toggle operations.

```
diagnose wad worker memcache toggle
```

diagnose wad worker memcache toggle all

Set/unset all operations as busy.

```
diagnose wad worker memcache toggle all [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker memcache toggle config

Toggle worker memcache config.

```
diagnose wad worker memcache toggle config [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker memcache toggle create

Toggle create as busy.

```
diagnose wad worker memcache toggle create [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker memcache toggle read

Toggle read as busy.

```
diagnose wad worker memcache toggle read [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker peer

Show peer statistics.

```
diagnose wad worker peer
```

diagnose wad worker peer clear

Clear peer statistics.

```
diagnose wad worker peer clear
```

diagnose wad worker peer list

List peer statistics.

```
diagnose wad worker peer list
```

diagnose wad worker policy

Show policy statistics.

```
diagnose wad worker policy
```

diagnose wad worker policy clear

Clear policy statistics.

```
diagnose wad worker policy clear
```

diagnose wad worker policy list

List policy statistics.

```
diagnose wad worker policy list
```

diagnose wad worker restart

Restart workers.

```
diagnose wad worker restart [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker saml

Show saml sessions and GrpSID cache info.

```
diagnose wad worker saml [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker scripts

Show scripts statistics.

```
diagnose wad worker scripts
```

diagnose wad worker scripts clear

Clear scripts statistics.

```
diagnose wad worker scripts clear
```

diagnose wad worker scripts list

List scripts statistics.

```
diagnose wad worker scripts list
```

diagnose wad worker webcache

Webcache diagnostics.

```
diagnose wad worker webcache
```

diagnose wad worker webcache clear

Purge all entries.

```
diagnose wad worker webcache clear [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache flush

Reset statistics.

```
diagnose wad worker webcache flush [<index>]
```


Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache stats

Show statistics.

```
diagnose wad worker webcache stats [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache summary

List statistics summary.

```
diagnose wad worker webcache summary
```

diagnose wad worker webcache toggle

Toggle operations.

```
diagnose wad worker webcache toggle
```

diagnose wad worker webcache toggle abort

Toggle abort as busy.

```
diagnose wad worker webcache toggle abort [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle add_ref

Toggle add_ref as busy.

```
diagnose wad worker webcache toggle add_ref [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle all

Set/unset all operations as busy.

```
diagnose wad worker webcache toggle all [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle append

Toggle append as busy.

```
diagnose wad worker webcache toggle append [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle config

Toggle worker webcache config.

```
diagnose wad worker webcache toggle config [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle create

Toggle create as busy.

```
diagnose wad worker webcache toggle create [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle read

Toggle read as busy.

```
diagnose wad worker webcache toggle read [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle remove

Toggle remove as busy.

```
diagnose wad worker webcache toggle remove [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle resolve

Toggle resolve as busy.

```
diagnose wad worker webcache toggle resolve [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker webcache toggle update

Toggle update as busy.

```
diagnose wad worker webcache toggle update [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wadbd

WAN accelerator DB daemon.

This topic includes the following commands:

- [diagnose wadbd clear on page 3572](#)
- [diagnose wadbd restart on page 3572](#)
- [diagnose wadbd stats on page 3572](#)

diagnose wadbd clear

Remove all entries from the database.

```
diagnose wadbd clear
```

diagnose wadbd restart

Restart the daemon and reset the statistical parameters.

```
diagnose wadbd restart
```

diagnose wadbd stats

Show statistics.

```
diagnose wadbd stats
```

diagnose waf

WAF diagnostics.

This topic includes the following commands:

- [diagnose waf dump on page 3573](#)
- [diagnose waf info on page 3573](#)

diagnose waf dump

Dump WAF name table.

```
diagnose waf dump
```

diagnose waf info

Init WAF name table.

```
diagnose waf info
```

diagnose webfilter bword

Web banned word match filter.

This topic includes the following commands:

- [diagnose webfilter bword matchfilter on page 3573](#)

diagnose webfilter bword matchfilter

Filtered list display.

```
diagnose webfilter bword matchfilter <filter string>
```

Parameter	Description	Type	Size
<filter string>	Filter string from end of web filter banned word log line. For example: '1-n8 4 0 1 4 10 nC 4'	string	

diagnose webfilter fortiguard

FortiGuard Web Filter information

This topic includes the following commands:

- [diagnose webfilter fortiguard cache on page 3574](#)
- [diagnose webfilter fortiguard cache dump on page 3574](#)
- [diagnose webfilter fortiguard cache obs on page 3574](#)

- [diagnose webfilter fortiguard cache prefix on page 3574](#)
- [diagnose webfilter fortiguard cache tree on page 3575](#)
- [diagnose webfilter fortiguard cache ttl on page 3575](#)
- [diagnose webfilter fortiguard override on page 3575](#)
- [diagnose webfilter fortiguard override all-admin-override on page 3575](#)
- [diagnose webfilter fortiguard override all-user-override on page 3575](#)
- [diagnose webfilter fortiguard override all-warning on page 3575](#)
- [diagnose webfilter fortiguard override obs on page 3576](#)
- [diagnose webfilter fortiguard override statistics on page 3576](#)
- [diagnose webfilter fortiguard statistics on page 3576](#)
- [diagnose webfilter fortiguard statistics flush on page 3576](#)
- [diagnose webfilter fortiguard statistics list on page 3576](#)

diagnose webfilter fortiguard cache

Display WF cache content.

```
diagnose webfilter fortiguard cache
```

diagnose webfilter fortiguard cache dump

Display WF cache contents.

```
diagnose webfilter fortiguard cache dump
```

diagnose webfilter fortiguard cache obs

Display WF cache OBS info.

```
diagnose webfilter fortiguard cache obs
```

diagnose webfilter fortiguard cache prefix

Display WF cache contents of prefix type.

```
diagnose webfilter fortiguard cache prefix
```

diagnose webfilter fortiguard cache tree

Display WF cache in tree format.

```
diagnose webfilter fortiguard cache tree
```

diagnose webfilter fortiguard cache ttl

Display WF cache TTL list.

```
diagnose webfilter fortiguard cache ttl
```

diagnose webfilter fortiguard override

Display override content.

```
diagnose webfilter fortiguard override
```

diagnose webfilter fortiguard override all-admin-override

Display admin override entries of all vdoms.

```
diagnose webfilter fortiguard override all-admin-override
```

diagnose webfilter fortiguard override all-user-override

Display user override entries of all vdoms.

```
diagnose webfilter fortiguard override all-user-override
```

diagnose webfilter fortiguard override all-warning

Display warning/authentication entries of all vdoms.

```
diagnose webfilter fortiguard override all-warning
```

diagnose webfilter fortiguard override obs

Display override cache OBS info.

```
diagnose webfilter fortiguard override obs
```

diagnose webfilter fortiguard override statistics

Display override cache statistics.

```
diagnose webfilter fortiguard override statistics
```

diagnose webfilter fortiguard statistics

Rating cache and daemon statistics.

```
diagnose webfilter fortiguard statistics
```

diagnose webfilter fortiguard statistics flush

Flush rating cache and daemon statistics.

```
diagnose webfilter fortiguard statistics flush
```

diagnose webfilter fortiguard statistics list

Display rating cache and daemon statistics.

```
diagnose webfilter fortiguard statistics list
```

diagnose webfilter quota

Urlfilter daemon quota information.

This topic includes the following commands:

- [diagnose webfilter quota list on page 3577](#)

diagnose webfilter quota list

Display urlfilter daemon quota list.

```
diagnose webfilter quota list
```

diagnose webfilter stats

Proxy and flow webfilter statistics.

This topic includes the following commands:

- [diagnose webfilter stats clear on page 3577](#)
- [diagnose webfilter stats list on page 3577](#)

diagnose webfilter stats clear

Clear webfilter statistics.

```
diagnose webfilter stats clear <vdname>
```

Parameter	Description	Type	Size
<vdname>	VDOM name or global.	string	

diagnose webfilter stats list

Display webfilter statistics.

```
diagnose webfilter stats list <vdname>
```

Parameter	Description	Type	Size
<vdname>	VDOM name or global.	string	

diagnose web-ui

Web user interface.

This topic includes the following commands:

- [diagnose web-ui api-cache on page 3578](#)
- [diagnose web-ui api-cache statistic on page 3578](#)
- [diagnose web-ui api-stats on page 3578](#)
- [diagnose web-ui api-stats disable on page 3579](#)
- [diagnose web-ui api-stats enable on page 3579](#)
- [diagnose web-ui api-stats list on page 3579](#)
- [diagnose web-ui api-stats reset on page 3579](#)
- [diagnose web-ui api-stats status on page 3579](#)
- [diagnose web-ui backtrace on page 3579](#)
- [diagnose web-ui backtrace clear on page 3580](#)
- [diagnose web-ui backtrace disable on page 3580](#)
- [diagnose web-ui backtrace enable on page 3580](#)
- [diagnose web-ui backtrace httpsd on page 3580](#)
- [diagnose web-ui backtrace status on page 3580](#)
- [diagnose web-ui cache on page 3581](#)
- [diagnose web-ui cache disable on page 3581](#)
- [diagnose web-ui cache enable on page 3581](#)
- [diagnose web-ui local-process-guard on page 3581](#)
- [diagnose web-ui local-process-guard disable on page 3581](#)
- [diagnose web-ui local-process-guard enable on page 3581](#)
- [diagnose web-ui local-process-guard status on page 3582](#)
- [diagnose web-ui localization on page 3582](#)
- [diagnose web-ui localization disable on page 3582](#)
- [diagnose web-ui localization enable on page 3582](#)

diagnose web-ui api-cache

shows statistics of REST API caching.

```
diagnose web-ui api-cache
```

diagnose web-ui api-cache statistic

Show REST API cache statistics.

```
diagnose web-ui api-cache statistic
```

diagnose web-ui api-stats

REST API performance statistics.

```
diagnose web-ui api-stats
```

diagnose web-ui api-stats disable

Disable REST API performance statistics.

```
diagnose web-ui api-stats disable
```

diagnose web-ui api-stats enable

Enable REST API performance statistics.

```
diagnose web-ui api-stats enable
```

diagnose web-ui api-stats list

List all REST API performance statistics.

```
diagnose web-ui api-stats list <api-uri>
```

Parameter	Description	Type	Size
<api-uri>	API access URI/prefix. (type.path.name.action)	string	

diagnose web-ui api-stats reset

Reset all REST API performance statistics.

```
diagnose web-ui api-stats reset
```

diagnose web-ui api-stats status

Status of REST API performance statistics.

```
diagnose web-ui api-stats status
```

diagnose web-ui backtrace

Web-ui backtrace.

```
diagnose web-ui backtrace
```

diagnose web-ui backtrace clear

Clear all backtrace log.

```
diagnose web-ui backtrace clear
```

diagnose web-ui backtrace disable

Disable web-ui backtrace.

```
diagnose web-ui backtrace disable
```

diagnose web-ui backtrace enable

Enable web-ui backtrace.

```
diagnose web-ui backtrace enable
```

diagnose web-ui backtrace httpsd

List all httpsd backtrace log.

```
diagnose web-ui backtrace httpsd <error|<pid>>
```

Parameter	Description	Type	Size
<error <pid>>	Details of httpsd backtrace log (error: httpsd error log, <number>: pid of request log).	string	

diagnose web-ui backtrace status

Status of web-ui backtrace.

```
diagnose web-ui backtrace status
```

diagnose web-ui cache

Enable/disable caching of static resources.

```
diagnose web-ui cache
```

diagnose web-ui cache disable

Disable caching of static resources.

```
diagnose web-ui cache disable
```

diagnose web-ui cache enable

Enable caching of static resources.

```
diagnose web-ui cache enable
```

diagnose web-ui local-process-guard

Enable/disable the REST API local process guard.

```
diagnose web-ui local-process-guard
```

diagnose web-ui local-process-guard disable

Disable the REST API local process guard.

```
diagnose web-ui local-process-guard disable
```

diagnose web-ui local-process-guard enable

Enable the REST API local process guard.

```
diagnose web-ui local-process-guard enable
```

diagnose web-ui local-process-guard status

View the status of the REST API local process guard.

```
diagnose web-ui local-process-guard status
```

diagnose web-ui localization

Enable/disable language localization.

```
diagnose web-ui localization
```

diagnose web-ui localization disable

Disable language localization.

```
diagnose web-ui localization disable
```

diagnose web-ui localization enable

Enable language localization.

```
diagnose web-ui localization enable
```

diagnose wireless-controller

Wireless controller.

This topic includes the following commands:

- [diagnose wireless-controller wlac](#) on page 3582
- [diagnose wireless-controller wlac_hlp](#) on page 3583

diagnose wireless-controller wlac

WLAN AC.

```
diagnose wireless-controller wlac <-c|-d|-k|-h> <value1> <value2> <value3> <value4> <value5>  
<value6> <value7> <value8> <value9> <value10> <value11> <value12>
```

Parameter	Description	Type	Size
<-c -d -k -h>	Control plane, data plane or help.	string	
<value1>	Value of command.	string	
<value2>	Value of command.	string	
<value3>	Value of command.	string	
<value4>	Value of command.	string	
<value5>	Value of command.	string	
<value6>	Value of command.	string	
<value7>	Value of command.	string	
<value8>	Value of command.	string	
<value9>	Value of command.	string	
<value10>	Value of command.	string	
<value11>	Value of command.	string	
<value12>	Value of command.	string	

diagnose wireless-controller wlac_hlp

WLAN AC HELPER.

```
diagnose wireless-controller wlac_hlp <-c|-h> <value1> <value2> <value3>
```

Parameter	Description	Type	Size
<-c -h>	Control plane or help.	string	
<value1>	Value of command.	string	
<value2>	Value of command.	string	
<value3>	Value of command.	string	

diagnose wpa

wpa daemon

This topic includes the following commands:

- [diagnose wpa wpaad on page 3584](#)

diagnose wpa wpad

wpad diagnostics.

```
diagnose wpa wpad <subcmd> <value1> <value2> <value3> <value4> <value5>
```

Parameter	Description	Type	Size
<subcmd>	sub command.	string	
<value1>	Value of command.	string	
<value2>	Value of command.	string	
<value3>	Value of command.	string	
<value4>	Value of command.	string	
<value5>	Value of command.	string	

CLI execute commands

Use execute commands to run system commands.

This section includes syntax for the following commands:

- [execute api-user on page 3587](#)
- [execute auto-script on page 3588](#)
- [execute azure on page 3590](#)
- [execute backup on page 3591](#)
- [execute batch on page 3602](#)
- [execute central-mgmt on page 3603](#)
- [execute cfg on page 3604](#)
- [execute clear-admin-password-history on page 3605](#)
- [execute clear-user-password-history on page 3605](#)
- [execute clear on page 3605](#)
- [execute cli on page 3606](#)
- [execute cloud-service on page 3606](#)
- [execute config-transaction on page 3607](#)
- [execute cpu on page 3608](#)
- [execute date on page 3609](#)
- [execute device-upgrade on page 3609](#)
- [execute dhcp on page 3610](#)
- [execute dhcp6 on page 3611](#)
- [execute disconnect-admin-session on page 3612](#)
- [execute disk on page 3612](#)
- [execute enter on page 3613](#)
- [execute erase-disk on page 3613](#)
- [execute extender on page 3613](#)
- [execute fabric-vpn on page 3618](#)
- [execute factoryreset-for-central-management on page 3619](#)
- [execute factoryreset-shutdown on page 3619](#)
- [execute factoryreset on page 3618](#)
- [execute factoryreset2 on page 3619](#)
- [execute fctems on page 3620](#)
- [execute federated-upgrade on page 3621](#)
- [execute fips on page 3623](#)
- [execute firewall on page 3623](#)
- [execute formatlogdisk on page 3624](#)
- [execute forticarrier-license on page 3624](#)
- [execute forticloud-sandbox on page 3625](#)

- [execute fortiguard-log on page 3625](#)
- [execute fortiguard-message on page 3626](#)
- [execute fortimanager on page 3627](#)
- [execute fortitoken-cloud on page 3630](#)
- [execute fortitoken-mobile on page 3632](#)
- [execute fortitoken on page 3627](#)
- [execute fsso on page 3633](#)
- [execute gen-token on page 3633](#)
- [execute ha on page 3634](#)
- [execute interface on page 3636](#)
- [execute internet-service4 on page 3637](#)
- [execute internet-service6 on page 3637](#)
- [execute ipam on page 3637](#)
- [execute iscsi on page 3638](#)
- [execute kmip on page 3639](#)
- [execute log on page 3640](#)
- [execute mem on page 3649](#)
- [execute mrouter on page 3650](#)
- [execute mrouter6 on page 3652](#)
- [execute nsx on page 3653](#)
- [execute oqs on page 3654](#)
- [execute ping-options on page 3658](#)
- [execute ping on page 3654](#)
- [execute ping6-options on page 3655](#)
- [execute ping6 on page 3654](#)
- [execute policy-packet-capture on page 3663](#)
- [execute reboot on page 3663](#)
- [execute replace-device on page 3663](#)
- [execute report-config on page 3665](#)
- [execute report on page 3664](#)
- [execute restore on page 3666](#)
- [execute revision on page 3675](#)
- [execute router on page 3676](#)
- [execute sdn-vpn on page 3679](#)
- [execute sdn on page 3679](#)
- [execute send-fds-statistics on page 3680](#)
- [execute send-fmg-list on page 3680](#)
- [execute set on page 3681](#)
- [execute shutdown on page 3687](#)
- [execute speed-test-custom on page 3688](#)
- [execute speed-test-ipsec on page 3688](#)
- [execute speed-test-options on page 3688](#)
- [execute speed-test-server on page 3692](#)

- [execute speed-test on page 3687](#)
- [execute ssh-options on page 3694](#)
- [execute ssh-regen-keys on page 3695](#)
- [execute ssh on page 3693](#)
- [execute ssh6-options on page 3693](#)
- [execute ssh6 on page 3693](#)
- [execute switch-controller on page 3695](#)
- [execute sync-IPSec on page 3713](#)
- [execute sync-session on page 3714](#)
- [execute system on page 3714](#)
- [execute tac on page 3715](#)
- [execute telnet-options on page 3715](#)
- [execute telnet on page 3715](#)
- [execute test on page 3716](#)
- [execute time on page 3717](#)
- [execute traceroute-options on page 3717](#)
- [execute traceroute on page 3717](#)
- [execute tracert6 on page 3719](#)
- [execute upd-vd-license on page 3721](#)
- [execute update-av on page 3719](#)
- [execute update-eip on page 3719](#)
- [execute update-external-resource on page 3720](#)
- [execute update-ffdb-on-demand on page 3720](#)
- [execute update-geo-ip on page 3720](#)
- [execute update-ips on page 3720](#)
- [execute update-now on page 3720](#)
- [execute update-src-vis on page 3721](#)
- [execute upload on page 3721](#)
- [execute vm-license-options on page 3724](#)
- [execute vm-license on page 3724](#)
- [execute vpn on page 3726](#)
- [execute wake-on-lan on page 3738](#)
- [execute webcache on page 3739](#)
- [execute webfilter on page 3740](#)
- [execute wireless-controller on page 3740](#)

execute api-user

api-user

This topic includes the following commands:

- [execute api-user generate-key on page 3588](#)

execute api-user generate-key

Generate key for API users.

```
execute api-user generate-key <name> <expiry>
```

Parameter	Description	Type	Size
<name>	API user name.	string	
<expiry>	Optional expiry of API key in minutes from now (valid range: 1 - 10080)	string	

execute auto-script

auto-script

This topic includes the following commands:

- [execute auto-script backup ftp on page 3588](#)
- [execute auto-script backup tftp on page 3589](#)
- [execute auto-script delete on page 3589](#)
- [execute auto-script result on page 3589](#)
- [execute auto-script start on page 3589](#)
- [execute auto-script status on page 3590](#)
- [execute auto-script stop on page 3590](#)
- [execute auto-script stopall on page 3590](#)

execute auto-script backup ftp

Backup output file to FTP sever.

```
execute auto-script backup ftp <name> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<name>	Script name.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	

Parameter	Description	Type	Size
<passwd>	FTP password.	string	

execute auto-script backup tftp

Backup output file to TFTP sever.

```
execute auto-script backup tftp <name> <tftp server>
```

Parameter	Description	Type	Size
<name>	Script name.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute auto-script delete

Delete output of executed scripts.

```
execute auto-script delete <name>
```

Parameter	Description	Type	Size
<name>	Script name.	string	

execute auto-script result

Display output of executed scripts.

```
execute auto-script result <name>
```

Parameter	Description	Type	Size
<name>	Script name.	string	

execute auto-script start

Start script.

```
execute auto-script start <name>
```

Parameter	Description	Type	Size
<name>	Script name.	string	

execute auto-script status

List of scripts currently running or executed.

```
execute auto-script status
```

execute auto-script stop

Stop script.

```
execute auto-script stop <name>
```

Parameter	Description	Type	Size
<name>	Script name.	string	

execute auto-script stopall

Stop all scripts currently running.

```
execute auto-script stopall
```

execute azure

azure

This topic includes the following commands:

- [execute azure vwan-payg-billing status on page 3590](#)
- [execute azure vwan-payg-billing usage on page 3591](#)
- [execute azure vwan-slb pull on page 3591](#)
- [execute azure vwan-slb show on page 3591](#)

execute azure vwan-payg-billing status

Display vwan payg billing status.

```
execute azure vwan-payg-billing status
```

execute azure vwan-payg-billing usage

Display all usage events that have been posted.

```
execute azure vwan-payg-billing usage
```

execute azure vwan-slb pull

Pull the Azure vWAN SLB online setting to local cmdb.

```
execute azure vwan-slb pull
```

execute azure vwan-slb show

Display the Azure vWAN SLB online setting.

```
execute azure vwan-slb show
```

execute backup

backup

This topic includes the following commands:

- [execute backup config flash on page 3592](#)
- [execute backup config ftp on page 3592](#)
- [execute backup config management-station on page 3593](#)
- [execute backup config sftp on page 3593](#)
- [execute backup config tftp on page 3593](#)
- [execute backup disk alllogs ftp on page 3594](#)
- [execute backup disk alllogs tftp on page 3594](#)
- [execute backup disk ipsarchives ftp on page 3594](#)
- [execute backup disk ipsarchives tftp on page 3594](#)
- [execute backup disk log ftp on page 3595](#)
- [execute backup disk log tftp on page 3595](#)
- [execute backup full-config ftp on page 3595](#)
- [execute backup full-config sftp on page 3596](#)
- [execute backup full-config tftp on page 3596](#)

- [execute backup ipsuserdefsig ftp on page 3597](#)
- [execute backup ipsuserdefsig tftp on page 3597](#)
- [execute backup memory alllogs ftp on page 3597](#)
- [execute backup memory alllogs tftp on page 3597](#)
- [execute backup memory log ftp on page 3598](#)
- [execute backup memory log tftp on page 3598](#)
- [execute backup obfuscated-config ftp on page 3598](#)
- [execute backup obfuscated-config management-station on page 3599](#)
- [execute backup obfuscated-config sftp on page 3599](#)
- [execute backup obfuscated-config tftp on page 3599](#)
- [execute backup obfuscated-full-config ftp on page 3600](#)
- [execute backup obfuscated-full-config sftp on page 3600](#)
- [execute backup obfuscated-full-config tftp on page 3601](#)
- [execute backup obfuscated-yaml-config ftp on page 3601](#)
- [execute backup obfuscated-yaml-config tftp on page 3601](#)
- [execute backup yaml-config ftp on page 3602](#)
- [execute backup yaml-config tftp on page 3602](#)

execute backup config flash

Backup config file to flash.

```
execute backup config flash <comment>
```

Parameter	Description	Type	Size
<comment>	Make a comment for this config backup.	string	

execute backup config ftp

Backup config file to FTP server.

```
execute backup config ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>  
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	

Parameter	Description	Type	Size
<passwd>	FTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup config management-station

Backup config file to management station.

```
execute backup config management-station <comment>
```

Parameter	Description	Type	Size
<comment>	Make a comment for this config backup.	string	

execute backup config sftp

Backup config file to SFTP server.

```
execute backup config sftp <string> <sftp server>[:sftp port] <user> <passwd> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the SFTP server.	string	
<sftp server>[:sftp port]	SFTP server IPv4, IPv6 can be attached with port.	string	
<user>	SFTP username.	string	
<passwd>	SFTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup config tftp

Backup config file to TFTP server.

```
execute backup config tftp <string> <tftp server> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup disk alllogs ftp

Backup all log files to FTP server.

```
execute backup disk alllogs ftp <ftp server>[:ftp port] <Enter>|<user> <passwd> <Enter>|<string>
```

Parameter	Description	Type	Size
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter> <string>	Optional log file compression option [uncompressed compressed].	string	

execute backup disk alllogs tftp

Backup all log file(s) to TFTP server.

```
execute backup disk alllogs tftp <tftp server>
```

Parameter	Description	Type	Size
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute backup disk ipsarchives ftp

Backup IPS archive file(s) to FTP server.

```
execute backup disk ipsarchives ftp <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute backup disk ipsarchives tftp

Backup IPS archive file(s) to TFTP server.

```
execute backup disk ipsarchives tftp <tftp server>
```

Parameter	Description	Type	Size
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute backup disk log ftp

Backup specific log file(s) to FTP server.

```
execute backup disk log ftp <ftp server>[:ftp port] <user> <passwd> <string> <Enter>|<string>
```

Parameter	Description	Type	Size
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<user>	FTP username.	string	
<passwd>	FTP password.	string	
<string>	, traffic, event, virus, webfilter, ips, emailfilter, anomaly, voip, dlp, app-ctrl, waf, gtp, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb, debug	string	
<Enter> <string>	Optional log file compression option [uncompressed compressed].	string	

execute backup disk log tftp

Backup specific log file(s) to TFTP server.

```
execute backup disk log tftp <tftp server> <string>
```

Parameter	Description	Type	Size
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<string>	, traffic, event, virus, webfilter, ips, emailfilter, anomaly, voip, dlp, app-ctrl, waf, gtp, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb, debug	string	

execute backup full-config ftp

Backup full config file to FTP server.

```
execute backup full-config ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup full-config sftp

Backup full config file to SFTP server.

```
execute backup full-config sftp <string> <sftp server>[:sftp port] <user> <passwd>
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the SFTP server.	string	
<sftp server>[:sftp port]	SFTP server IPv4, IPv6 can be attached with port.	string	
<user>	SFTP username.	string	
<passwd>	SFTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup full-config tftp

Backup full config file to TFTP server.

```
execute backup full-config tftp <string> <tftp server> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup ipsuserdefsig ftp

Backup user defined IPS signatures to FTP server.

```
execute backup ipsuserdefsig ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute backup ipsuserdefsig tftp

Backup user defined IPS signatures to TFTP server.

```
execute backup ipsuserdefsig tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute backup memory alllogs ftp

Backup all log files to FTP server.

```
execute backup memory alllogs ftp <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute backup memory alllogs tftp

Backup all log file(s) to TFTP server.

```
execute backup memory alllogs tftp <tftp server>
```

Parameter	Description	Type	Size
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute backup memory log ftp

Backup specific log file(s) to FTP server.

```
execute backup memory log ftp <ftp server>[:ftp port] <user> <passwd> <string>
```

Parameter	Description	Type	Size
<ftp server> [:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<user>	FTP username.	string	
<passwd>	FTP password.	string	
<string>	, traffic, event, virus, webfilter, ips, emailfilter, anomaly, voip, dlp, app-ctrl, waf, gtp, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb, debug	string	

execute backup memory log tftp

Backup specific log file(s) to TFTP server.

```
execute backup memory log tftp <tftp server> <string>
```

Parameter	Description	Type	Size
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<string>	, traffic, event, virus, webfilter, ips, emailfilter, anomaly, voip, dlp, app-ctrl, waf, gtp, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb, debug	string	

execute backup obfuscated-config ftp

Backup obfuscated config file to FTP server.

```
execute backup obfuscated-config ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>  
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup obfuscated-config management-station

Backup obfuscated config file to management station.

```
execute backup obfuscated-config management-station <comment>
```

Parameter	Description	Type	Size
<comment>	Make a comment for this config backup.	string	

execute backup obfuscated-config sftp

Backup obfuscated config file to SFTP server.

```
execute backup obfuscated-config sftp <string> <sftp server>[:sftp port] <user> <passwd>
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the SFTP server.	string	
<sftp server>[:sftp port]	SFTP server IPv4, IPv6 can be attached with port.	string	
<user>	SFTP username.	string	
<passwd>	SFTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup obfuscated-config tftp

Backup obfuscated config file to TFTP server.

```
execute backup obfuscated-config tftp <string> <tftp server> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup obfuscated-full-config ftp

Backup obfuscated full config file to FTP server.

```
execute backup obfuscated-full-config ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup obfuscated-full-config sftp

Backup obfuscated full config file to SFTP server.

```
execute backup obfuscated-full-config sftp <string> <sftp server>[:sftp port] <user> <passwd>
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the SFTP server.	string	
<sftp server>[:sftp port]	SFTP server IPv4, IPv6 can be attached with port.	string	
<user>	SFTP username.	string	
<passwd>	SFTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup obfuscated-full-config tftp

Backup obfuscated full config file to TFTP server.

```
execute backup obfuscated-full-config tftp <string> <tftp server> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup obfuscated-yaml-config ftp

Backup obfuscated YAML config file to FTP server.

```
execute backup obfuscated-yaml-config ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>  
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup obfuscated-yaml-config tftp

Backup obfuscated YAML config file to TFTP server.

```
execute backup obfuscated-yaml-config tftp <string> <tftp server> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup yaml-config ftp

Backup YAML config file to FTP server.

```
execute backup yaml-config ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>  
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup yaml-config tftp

Backup YAML config file to TFTP server.

```
execute backup yaml-config tftp <string> <tftp server> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name (path) on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute batch

batch

This topic includes the following commands:

- [execute batch end on page 3603](#)
- [execute batch lastlog on page 3603](#)
- [execute batch start on page 3603](#)
- [execute batch status on page 3603](#)

execute batch end

Batch mode end.

```
execute batch end
```

execute batch lastlog

Read the result of last batch commands.

```
execute batch lastlog
```

execute batch start

Batch mode start.

```
execute batch start
```

execute batch status

Batch mode status.

```
execute batch status
```

execute central-mgmt

central-mgmt

This topic includes the following commands:

- [execute central-mgmt register-device on page 3603](#)
- [execute central-mgmt set-mgmt-id on page 3604](#)
- [execute central-mgmt unregister-device on page 3604](#)

execute central-mgmt register-device

Register device to FortiManager from unregistered device list.

```
execute central-mgmt register-device <fmg-serial-no> <fmg-register-password>
```

Parameter	Description	Type	Size
<fmg-serial-no>	FortiManager serial number.	string	
<fmg-register-password>	Register password in to FortiManager.	string	

execute central-mgmt set-mgmt-id

Management ID of Central Management Service.

```
execute central-mgmt set-mgmt-id <management id>
```

Parameter	Description	Type	Size
<management id>	Management ID (must be entered in encrypted format).	string	

execute central-mgmt unregister-device

Remove device from its manager's device list.

```
execute central-mgmt unregister-device <fmg-serial-no>
```

Parameter	Description	Type	Size
<fmg-serial-no>	FortiManager serial number.	string	

execute cfg

cfg

This topic includes the following commands:

- [execute cfg reload on page 3604](#)
- [execute cfg save on page 3605](#)

execute cfg reload

Reboot to reload the configs.

```
execute cfg reload
```

execute cfg save

Save configs.

```
execute cfg save
```

execute clear

clear

This topic includes the following commands:

- [execute clear system arp table on page 3605](#)

execute clear system arp table

Clear system ARP table.

```
execute clear system arp table
```

execute clear-admin-password-history

Clear admin user password history.

```
execute clear-admin-password-history <admin user>
```

Parameter	Description	Type	Size
<admin user>	Name of admin user	string	

execute clear-user-password-history

Clear auth user password history.

```
execute clear-user-password-history <auth user>
```

Parameter	Description	Type	Size
<auth user>	Name of auth user	string	

execute cli

cli

This topic includes the following commands:

- [execute cli check-template-status on page 3606](#)
- [execute cli status-msg-only on page 3606](#)

execute cli check-template-status

Check SCP script template running status.

```
execute cli check-template-status
```

execute cli status-msg-only

CLI standardized error output.

```
execute cli status-msg-only <enable/disable>
```

Parameter	Description	Type	Size
<enable/disable>	Enable/disable CLI standardized error output.	string	

execute cloud-service

cloud-service

This topic includes the following commands:

- [execute cloud-service gen-jwt-as-token on page 3607](#)
- [execute cloud-service list on page 3607](#)
- [execute cloud-service manual-gen-jwt-as-token on page 3607](#)

execute cloud-service gen-jwt-as-token

Generate a JSON Web Token from config to be used as bearer token.

```
execute cloud-service gen-jwt-as-token <string>
```

Parameter	Description	Type	Size
<string>	Cloud service name.	string	

execute cloud-service list

List cloud service information.

```
execute cloud-service list <string>
```

Parameter	Description	Type	Size
<string>	Cloud service name.	string	

execute cloud-service manual-gen-jwt-as-token

Manually generate a JSON Web Token to be used as bearer token.

```
execute cloud-service manual-gen-jwt-as-token <string> <string> <string> <string> <integer> <integer>
```

Parameter	Description	Type	Size
<string>	keyid.	string	
<string>	private key in clear text, consider quoting everything in ``, as `\\n` needs to be transcoded as a real new line.	string	
<string>	issuer.	string	
<string>	subject.	string	
<integer>	token in effective starting from (epoch seconds).	string	
<integer>	token lifetime (seconds).	string	

execute config-transaction

config-transaction

This topic includes the following commands:

- [execute config-transaction abort on page 3608](#)
- [execute config-transaction commit on page 3608](#)
- [execute config-transaction start on page 3608](#)

execute config-transaction abort

Abort configuration transaction.

```
execute config-transaction abort
```

execute config-transaction commit

Commit configuration transaction.

```
execute config-transaction commit
```

execute config-transaction start

Start configuration transaction.

```
execute config-transaction start <integer>
```

Parameter	Description	Type	Size
<integer>	Transaction timeout in minutes (1 - 60). Default value is 5.	string	

execute cpu

cpu

This topic includes the following commands:

- [execute cpu add on page 3608](#)
- [execute cpu show on page 3609](#)

execute cpu add

Activate new CPU.


```
execute cpu add <number>
```

Parameter	Description	Type	Size
<number>	New Active CPU Number.	string	

execute cpu show

Show CPU number.

```
execute cpu show
```

execute date

System date.

```
execute date <yyyy-mm-dd>
```

Parameter	Description	Type	Size
<yyyy-mm-dd>	yyyy: 2001-2037, mm: 1-12, dd: 1-31.	string	

execute device-upgrade

device-upgrade

This topic includes the following commands:

- [execute device-upgrade cancel on page 3609](#)
- [execute device-upgrade immediate on page 3610](#)

execute device-upgrade cancel

Cancel a Fortinet device's upgrade by removing it from the upgrade table.

```
execute device-upgrade cancel <serial>
```

Parameter	Description	Type	Size
<serial>	Serial number of the Fortinet device to upgrade.	string	

execute device-upgrade immediate

Configure a Fortinet device to upgrade immediately.

```
execute device-upgrade immediate <device-type> <serial> <major> <minor> <patch>
```

Parameter	Description	Type	Size
<device-type>	Fortinet device type to upgrade.	string	
<serial>	Fortinet device serial number to upgrade.	string	
<major>	Major version of the Fortinet OS image being upgraded to.	string	
<minor>	Minor version of the Fortinet OS image being upgraded to.	string	
<patch>	Patch version of the Fortinet OS image being upgraded to.	string	

execute dhcp

dhcp

This topic includes the following commands:

- [execute dhcp lease-clear on page 3610](#)
- [execute dhcp lease-list on page 3611](#)

execute dhcp lease-clear

Clear all DHCP leases.

```
execute dhcp lease-clear <IPv4 address> or <IPv4 starting address-IPv4 ending address> <all>
```

Parameter	Description	Type	Size
<IPv4 address> or <IPv4 starting address-IPv4 ending address>	Clear lease(s) on this IP address.	string	
<all>	Clear all leases.	string	

execute dhcp lease-list

List all DHCP leases.

```
execute dhcp lease-list <interface>
```

Parameter	Description	Type	Size
<interface>	List leases on this interface.	string	

execute dhcp6

dhcp6

This topic includes the following commands:

- [execute dhcp6 lease-clear on page 3611](#)
- [execute dhcp6 lease-list on page 3611](#)

execute dhcp6 lease-clear

Clear all DHCPv6 leases.

```
execute dhcp6 lease-clear <IPv6 address> or <IPv6 starting address-IPv6 ending address> <all>
```

Parameter	Description	Type	Size
<IPv6 address> or <IPv6 starting address-IPv6 ending address>	Clear lease(s) on this IPv6 address.	string	
<all>	Clear all leases.	string	

execute dhcp6 lease-list

List all DHCPv6 leases.

```
execute dhcp6 lease-list <interface>
```

Parameter	Description	Type	Size
<interface>	List leases on this interface.	string	

execute disconnect-admin-session

Disconnect logged-in admin user.

```
execute disconnect-admin-session <integer>
```

Parameter	Description	Type	Size
<integer>	Index of user to be disconnected in logged-users table.	string	

execute disk

disk

This topic includes the following commands:

- [execute disk format on page 3612](#)
- [execute disk list on page 3612](#)
- [execute disk scan on page 3612](#)

execute disk format

Format a partition.

```
execute disk format
```

execute disk list

List disk devices and partitions.

```
execute disk list
```

execute disk scan

Scan a partition and fix errors.

```
execute disk scan
```

execute enter

Select virtual domain.

```
execute enter <name>
```

Parameter	Description	Type	Size
<name>	VDOM name.	string	

execute erase-disk

Erase a disk.

```
execute erase-disk
```

execute extender

extender

This topic includes the following commands:

- [execute extender delete-fortiextender-image on page 3614](#)
- [execute extender install-forticloud-mdm-package on page 3614](#)
- [execute extender install-forticloud-os-image on page 3614](#)
- [execute extender list-fortiextender-image on page 3614](#)
- [execute extender lte-carrier add on page 3614](#)
- [execute extender lte-carrier del on page 3615](#)
- [execute extender lte-simmap add on page 3615](#)
- [execute extender lte-simmap del on page 3615](#)
- [execute extender push-fortiextender-image on page 3616](#)
- [execute extender push-fortiextender-stage-image on page 3616](#)
- [execute extender query-forticloud-mdmpkg-image on page 3616](#)
- [execute extender query-forticloud-os-image on page 3617](#)
- [execute extender reset-fortiextender on page 3617](#)
- [execute extender restart-fortiextender-daemon on page 3617](#)

- [execute extender upload-fortiextender-image ftp](#) on page 3617
- [execute extender upload-fortiextender-image tftp](#) on page 3618

execute extender delete-fortiextender-image

Delete FortiExtender images.

```
execute extender delete-fortiextender-image
```

execute extender install-forticloud-mdm-package

Install FortiExtender modem package from Cloud.

```
execute extender install-forticloud-mdm-package <filename> <sn>
```

Parameter	Description	Type	Size
<filename>	FortiExtender Cloud modem package version.	string	
<sn>	FortiExtender serial number.	string	

execute extender install-forticloud-os-image

Install FortiExtender OS image from Cloud.

```
execute extender install-forticloud-os-image <filename> <sn>
```

Parameter	Description	Type	Size
<filename>	FortiExtender Cloud image version.	string	
<sn>	FortiExtender serial number.	string	

execute extender list-fortiextender-image

List FortiExtender images.

```
execute extender list-fortiextender-image
```

execute extender lte-carrier add

Add a LTE carrier with string.

```
execute extender lte-carrier add <SN> <string> [<string>]
```

Parameter	Description	Type	Size
<SN>	FortiExtender serial number.	string	
<string>	Newly added carrier name on the FEXT.	string	
[<string>]	Optional and default as GENERIC. Base carrier name on the FEXT, where the PRI and FW is referred by the newly added carrier.	string	

execute extender lte-carrier del

Delete a LTE carrier with string.

```
execute extender lte-carrier del <SN> <string>
```

Parameter	Description	Type	Size
<SN>	FortiExtender serial number.	string	
<string>	Carrier name on the FEXT.	string	

execute extender lte-simmap add

Add a carrier based on MCC/MNC.

```
execute extender lte-simmap add <SN> <string> <string> <string>
```

Parameter	Description	Type	Size
<SN>	FortiExtender serial number.	string	
<string>	MCC number.	string	
<string>	MNC number.	string	
<string>	Carrier name on the FEXT.	string	

execute extender lte-simmap del

Delete a LTE carrier with string.

```
execute extender lte-simmap del <SN> <string> <string> <string>
```

Parameter	Description	Type	Size
<SN>	FortiExtender serial number.	string	
<string>	MCC number.	string	
<string>	MNC number.	string	
<string>	Carrier name on the FEXT.	string	

execute extender push-fortiextender-image

Push FortiExtender image to a managed FortiExtender.

```
execute extender push-fortiextender-image <vdom> <sn> <filename>
```

Parameter	Description	Type	Size
<vdom>	FortiExtender session VDOM.	string	
<sn>	FortiExtender serial number.	string	
<filename>	FortiExtender image filename.	string	

execute extender push-fortiextender-stage-image

Push FortiExtender stage image to a managed FortiExtender.

```
execute extender push-fortiextender-stage-image <vdom> <sn> <filename>
```

Parameter	Description	Type	Size
<vdom>	FortiExtender session VDOM.	string	
<sn>	FortiExtender serial number.	string	
<filename>	FortiExtender image filename.	string	

execute extender query-forticloud-mdmpkg-image

Query FortiExtender modem packages on Cloud.

```
execute extender query-forticloud-mdmpkg-image <all>|<filename> <sn>
```

Parameter	Description	Type	Size
<all> <filename>	FortiExtender Cloud modem packages.	string	
<sn>	FortiExtender serial number.	string	

execute extender query-forticloud-os-image

Query FortiExtender OS images on Cloud.

```
execute extender query-forticloud-os-image <all>|<filename> <sn>
```

Parameter	Description	Type	Size
<all> <filename>	FortiExtender Cloud OS images.	string	
<sn>	FortiExtender serial number.	string	

execute extender reset-fortiextender

Restart managed FortiExtender.

```
execute extender reset-fortiextender <all>|<SN>
```

Parameter	Description	Type	Size
<all> <SN>	FortiExtender serial number.	string	

execute extender restart-fortiextender-daemon

Restart ForExtender AC daemon.

```
execute extender restart-fortiextender-daemon
```

execute extender upload-fortiextender-image ftp

Upload FortiExtender image from FTP server.

```
execute extender upload-fortiextender-image ftp <string> <ftp server>[:ftp port] <Enter>|<user>  
<passwd>
```

Parameter	Description	Type	Size
<string>	FortiExtender image file name on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute extender upload-fortiextender-image tftp

Upload FortiExtender image from TFTP server.

```
execute extender upload-fortiextender-image tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute fabric-vpn

fabric-vpn

This topic includes the following commands:

- [execute fabric-vpn flush-setup on page 3618](#)
- [execute fabric-vpn update-setup on page 3618](#)

execute fabric-vpn flush-setup

Remove fabric VPN settings.

```
execute fabric-vpn flush-setup
```

execute fabric-vpn update-setup

Update fabric VPN setup.

```
execute fabric-vpn update-setup
```

execute factoryreset

Reset to factory default now.

```
execute factoryreset <keepvmlicense>
```

Parameter	Description	Type	Size
<keepvmlicense>	Keep VM license.	string	

execute factoryreset2

Reset to factory default except system.global.vdom-mode/system.global.long-vdom-name/VDOMS/system.virtual-switch/system.interface/system.settings/router.static/router.static6.

```
execute factoryreset2 <keepvmlicense>
```

Parameter	Description	Type	Size
<keepvmlicense>	Keep VM license.	string	

execute factoryreset-for-central-management

Reset to factory default except system.central-management.serial-number/system.central-management.fmg.

```
execute factoryreset-for-central-management <keepvmlicense>
```

Parameter	Description	Type	Size
<keepvmlicense>	Keep VM license.	string	

execute factoryreset-shutdown

Reset to factory default and shutdown.

```
execute factoryreset-shutdown <keepvmlicense>
```

Parameter	Description	Type	Size
<keepvmlicense>	Keep VM license.	string	

execute fctems

fctems

This topic includes the following commands:

- [execute fctems is-verified on page 3620](#)
- [execute fctems unverify on page 3620](#)
- [execute fctems verify on page 3620](#)

execute fctems is-verified

Check if Configured EMS server has a verified certificate.

```
execute fctems is-verified <fctems>
```

Parameter	Description	Type	Size
<fctems>	FortiClient EMS table entry id in CMDB.	string	

execute fctems unverify

Unverify FortiClient EMS server.

```
execute fctems unverify <fctems>
```

Parameter	Description	Type	Size
<fctems>	FortiClient EMS table entry id in CMDB.	string	

execute fctems verify

Verify FortiClient EMS server.

```
execute fctems verify <fctems>
```

Parameter	Description	Type	Size
<fctems>	FortiClient EMS table entry id in CMDB.	string	

execute federated-upgrade

federated-upgrade

This topic includes the following commands:

- [execute federated-upgrade cancel on page 3621](#)
- [execute federated-upgrade initialize on page 3621](#)
- [execute federated-upgrade quick-fortigate-upgrade on page 3621](#)
- [execute federated-upgrade quick-full-upgrade on page 3622](#)
- [execute federated-upgrade restart on page 3622](#)
- [execute federated-upgrade safe-cancel on page 3622](#)
- [execute federated-upgrade status on page 3622](#)

execute federated-upgrade cancel

Cancel the currently configured upgrade.

```
execute federated-upgrade cancel
```

execute federated-upgrade initialize

Set up a federated upgrade.

```
execute federated-upgrade initialize
```

execute federated-upgrade quick-fortigate-upgrade

Set up a 15 minute immediate mode upgrade for all FortiGates in the CSF tree.

```
execute federated-upgrade quick-fortigate-upgrade <major> <minor> <patch> <delay-minutes> <max-minutes>
```

Parameter	Description	Type	Size
<major>	Major version of the Fortinet OS image being upgraded to.	string	
<minor>	Minor version of the Fortinet OS image being upgraded to.	string	
<patch>	Patch version of the Fortinet OS image being upgraded to.	string	
<delay-minutes>	Minutes to delay before starting the upgrade setup.	string	

Parameter	Description	Type	Size
<max-minutes>	Number of minutes allowed for upgrade preparation.	string	

execute federated-upgrade quick-full-upgrade

Set up a 15 minute immediate mode upgrade for all CSF devices.

```
execute federated-upgrade quick-full-upgrade <major> <minor> <patch> <delay-minutes> <max-minutes>
```

Parameter	Description	Type	Size
<major>	Major version of the Fortinet OS image being upgraded to.	string	
<minor>	Minor version of the Fortinet OS image being upgraded to.	string	
<patch>	Patch version of the Fortinet OS image being upgraded to.	string	
<delay-minutes>	Minutes to delay before starting the upgrade setup.	string	
<max-minutes>	Number of minutes allowed for upgrade preparation.	string	

execute federated-upgrade restart

Restart the currently configured federated upgrade.

```
execute federated-upgrade restart
```

execute federated-upgrade safe-cancel

Cancel the currently configured upgrade via the safe cancel API. Only cancels user-created upgrades.

```
execute federated-upgrade safe-cancel
```

execute federated-upgrade status

Show the current status of federated upgrade.

```
execute federated-upgrade status
```

execute fips

fips

This topic includes the following commands:

- [execute fips tftp-drbg-entropy-source on page 3623](#)
- [execute fips tftp-test-vectors on page 3623](#)

execute fips tftp-drbg-entropy-source

tftp files and generate drbg entropy source samples

```
execute fips tftp-drbg-entropy-source <ip> <dir> <number> <number>
```

Parameter	Description	Type	Size
<ip>	IP address of the tftp server	string	
<dir>	directory for the entropy sample files	string	
<number>	samples size.	string	
<number>	total number of samples.	string	

execute fips tftp-test-vectors

tftp files and generate test vector results

```
execute fips tftp-test-vectors <ip> <dir> <file name>
```

Parameter	Description	Type	Size
<ip>	IP address of the tftp server	string	
<dir>	directory of the test files	string	
<file name>	The JSON file to test.	string	

execute firewall

firewall

This topic includes the following commands:

- [execute firewall ssh generate local-ca on page 3624](#)
- [execute firewall ssh generate local-key on page 3624](#)

execute firewall ssh generate local-ca

Generate the default ssh local key.

```
execute firewall ssh generate local-ca <string>
```

Parameter	Description	Type	Size
<string>	Local CA name.	string	

execute firewall ssh generate local-key

Generate the default ssh local key.

```
execute firewall ssh generate local-key <string>
```

Parameter	Description	Type	Size
<string>	Local key name.	string	

execute formatlogdisk

Format log disk.

```
execute formatlogdisk
```

execute forticarrier-license

forticarrier-license

```
execute forticarrier-license <activation-code>
```

Parameter	Description	Type	Size
<activation-code>	Format:0000-0000-0000-0000-0001 or <license-key> Format:0000-0000-0000-0000-0000-0000-00	string	

execute forticloud-sandbox

forticloud-sandbox

This topic includes the following commands:

- [execute forticloud-sandbox region on page 3625](#)
- [execute forticloud-sandbox update on page 3625](#)

execute forticloud-sandbox region

Get FortiCloud sandbox region.

```
execute forticloud-sandbox region
```

execute forticloud-sandbox update

Update FortiCloud sandbox contract.

```
execute forticloud-sandbox update
```

execute fortiguard-log

fortiguard-log

This topic includes the following commands:

- [execute fortiguard-log certificate-activation on page 3625](#)
- [execute fortiguard-log migration on page 3626](#)
- [execute fortiguard-log update on page 3626](#)

execute fortiguard-log certificate-activation

Activate FortiCloud certification.

```
execute fortiguard-log certificate-activation <code>
```

Parameter	Description	Type	Size
<code>	Activation code.	string	

execute fortiguard-log migration

Migrate standalone FortiGate Cloud account to FortiCloud.

```
execute fortiguard-log migration <password>
```

Parameter	Description	Type	Size
<password>	Password.	string	

execute fortiguard-log update

Update FortiCloud Contract.

```
execute fortiguard-log update
```

execute fortiguard-message

fortiguard-message

This topic includes the following commands:

- [execute fortiguard-message add on page 3626](#)
- [execute fortiguard-message info on page 3626](#)
- [execute fortiguard-message update on page 3627](#)

execute fortiguard-message add

Add FortiGuard Message Service activation code.

```
execute fortiguard-message add <activation code>
```

Parameter	Description	Type	Size
<activation code>	Activation code for FortiGuard Message Service.	string	

execute fortiguard-message info

Show info about FortiGuard Message Service.

```
execute fortiguard-message info
```

execute fortiguard-message update

Force to update FortiGuard Message Service.

```
execute fortiguard-message update
```

execute fortimanager

fortimanager

This topic includes the following commands:

- [execute fortimanager fetch on page 3627](#)
- [execute fortimanager register on page 3627](#)

execute fortimanager fetch

Fetch and verify the FortiManager certificate

```
execute fortimanager fetch
```

execute fortimanager register

Register Fortigate to Fortimanager

```
execute fortimanager register <ip>
```

Parameter	Description	Type	Size
<ip>	Fortimanager's ip that Fortigate will register to	string	

execute fortitoken

fortitoken

This topic includes the following commands:

- [execute fortitoken activate on page 3628](#)
- [execute fortitoken import ftp on page 3629](#)
- [execute fortitoken import tftp on page 3629](#)
- [execute fortitoken import usb on page 3629](#)
- [execute fortitoken import-sn-file on page 3629](#)
- [execute fortitoken sync on page 3630](#)

execute fortitoken activate

Activate FortiToken(s) with FortiGuard.

```
execute fortitoken activate <id> <id> <id> <id> <id> <id> <id> <id> <id> <id> <id> <id> <id> <id> <id> <id> <id>
```

Parameter	Description	Type	Size
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	
<id>	FortiToken ID.	string	

execute fortitoken import ftp

Import FortiToken seeds file from FTP server.

```
execute fortitoken import ftp <file name> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<file name>	FortiToken seeds file name.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute fortitoken import tftp

Import FortiToken seeds file from TFTP server.

```
execute fortitoken import tftp <file name> <tftp server>
```

Parameter	Description	Type	Size
<file name>	FortiToken seeds file name.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute fortitoken import usb

Import FortiToken seeds file from USB drive.

```
execute fortitoken import usb <file name>
```

Parameter	Description	Type	Size
<file name>	FortiToken seeds file name.	string	

execute fortitoken import-sn-file

Import FTK_200 serial number from FortiCare.

```
execute fortitoken import-sn-file <FTK_200 Serial Number>
```

Parameter	Description	Type	Size
<FTK_200 Serial Number>	FTK_200 serial number.	string	

execute fortitoken sync

Synchronize FortiToken by adjusting for drift of internal clock.

```
execute fortitoken sync <id> <code> <next code>
```

Parameter	Description	Type	Size
<id>	FortiToken ID.	string	
<code>	FortiToken code.	string	
<next code>	Next FortiToken code.	string	

execute fortitoken-cloud

fortitoken-cloud

This topic includes the following commands:

- [execute fortitoken-cloud migrate-ftm on page 3630](#)
- [execute fortitoken-cloud new on page 3631](#)
- [execute fortitoken-cloud show on page 3631](#)
- [execute fortitoken-cloud sync on page 3631](#)
- [execute fortitoken-cloud trial on page 3631](#)
- [execute fortitoken-cloud update on page 3631](#)

execute fortitoken-cloud migrate-ftm

Migrate FortiToken service to FortiToken Cloud.

```
execute fortitoken-cloud migrate-ftm <license number> <vdom>
```

Parameter	Description	Type	Size
<license number>	FortiToken mobile license number.	string	
<vdom>	VDOM name.	string	

execute fortitoken-cloud new

Send new activation code for a user.

```
execute fortitoken-cloud new <user name> <user type> <vdom>
```

Parameter	Description	Type	Size
<user name>	User name for new token.	string	
<user type>	Enter admin, local or remote.	string	
<vdom>	VDOM name.	string	

execute fortitoken-cloud show

Show service status of this FortiGate.

```
execute fortitoken-cloud show
```

execute fortitoken-cloud sync

Synchronize users to FortiToken Cloud.

```
execute fortitoken-cloud sync <user type>
```

Parameter	Description	Type	Size
<user type>	Enter <return>, all, local or remote.	string	

execute fortitoken-cloud trial

Activate free trial.

```
execute fortitoken-cloud trial
```

execute fortitoken-cloud update

Update VDOM list to FortiToken Cloud.

```
execute fortitoken-cloud update
```

execute fortitoken-mobile

fortitoken-mobile

This topic includes the following commands:

- [execute fortitoken-mobile import on page 3632](#)
- [execute fortitoken-mobile poll on page 3632](#)
- [execute fortitoken-mobile provision on page 3632](#)
- [execute fortitoken-mobile renew on page 3632](#)

execute fortitoken-mobile import

Import a list of tokens from FortiGuard to the FortiGate unit.

```
execute fortitoken-mobile import <code>
```

Parameter	Description	Type	Size
<code>	Software Token Redemption Certificate.	string	

execute fortitoken-mobile poll

Poll soft token states.

```
execute fortitoken-mobile poll
```

execute fortitoken-mobile provision

Provision a soft token.

```
execute fortitoken-mobile provision <sn>
```

Parameter	Description	Type	Size
<sn>	MobileToken serial number.	string	

execute fortitoken-mobile renew

Renew a locked mobile FortiToken.

```
execute fortitoken-mobile renew <sn>
```


Parameter	Description	Type	Size
<sn>	MobileToken serial number.	string	

execute fsso

fsso

This topic includes the following commands:

- [execute fsso refresh on page 3633](#)

execute fsso refresh

Refresh FSSO groups.

```
execute fsso refresh
```

execute gen-token

Generate bearer token.

```
execute gen-token <Type> <string> <Algorithm> <Expire>
```

Parameter	Description	Type	Size
<Type>	Type for token generation, by certificate or by pre-shared key. Available types: cert, key	string	
<string>	Certificate or preshared-key for token generation. Available certificates:	string	
<Algorithm>	Algorithm for token generation. Please ensure that the signing algorithm matches the type of certificate and its corresponding private key. Available Algorithms: RS256, RS384, RS512, ES256, ES384, ES512 for cert. HS256, HS384, HS512 for key.	string	
<Expire>	Expire interval in hours, 0 for long live token.	string	

execute ha

ha

This topic includes the following commands:

- [execute ha disconnect on page 3634](#)
- [execute ha failover set on page 3634](#)
- [execute ha failover status on page 3635](#)
- [execute ha failover unset on page 3635](#)
- [execute ha manage on page 3635](#)
- [execute ha synchronize on page 3635](#)

execute ha disconnect

Disconnect from HA cluster.

```
execute ha disconnect <string> <string> <ip> <netmask>
```

Parameter	Description	Type	Size
<string>	Serial number.	string	
<string>	Interface name.	string	
<ip>	IP or subnet of the interface.	string	
<netmask>	Netmask of the interface.	string	

execute ha failover set

Set the given virtual cluster as secondary and trigger failover. Argument optional; if argument omitted, all virtual clusters are affected.

```
execute ha failover set [integer]
```

Parameter	Description	Type	Size
[integer]	Virtual cluster ID. Optional; if not given, all virtual clusters are affected.	string	

execute ha failover status

Display whether the given virtual cluster has been set as secondary for failover. Argument optional; if no argument given, display statuses of all virtual clusters.

```
execute ha failover status [integer]
```

Parameter	Description	Type	Size
[integer]	Virtual cluster ID. Optional; if not given, all virtual clusters are affected.	string	

execute ha failover unset

If the given virtual cluster has been set as secondary before, unset it so HA will use normal criteria to decide the primary. May trigger a failover. Argument optional; if argument not given, all virtual clusters are affected.

```
execute ha failover unset [integer]
```

Parameter	Description	Type	Size
[integer]	Virtual cluster ID. Optional; if not given, all virtual clusters are affected.	string	

execute ha manage

HA cluster index.

```
execute ha manage <string> <string>
```

Parameter	Description	Type	Size
<string>	HA cluster index.	string	
<string>	Login admin name.	string	

execute ha synchronize

HA synchronize commands.

```
execute ha synchronize <string>
```

Parameter	Description	Type	Size
<string>	File type.	string	

execute interface

interface

This topic includes the following commands:

- [execute interface dhcp6client-renew on page 3636](#)
- [execute interface dhcpclient-renew on page 3636](#)
- [execute interface pppoe-reconnect on page 3636](#)

execute interface dhcp6client-renew

Renew DHCPv6 lease.

```
execute interface dhcp6client-renew <interface>
```

Parameter	Description	Type	Size
<interface>	Renew DHCPv6 lease on this interface.	string	

execute interface dhcpclient-renew

Renew DHCP lease.

```
execute interface dhcpclient-renew <interface>
```

Parameter	Description	Type	Size
<interface>	Renew DHCP lease on this interface.	string	

execute interface pppoe-reconnect

Reconnect to PPPoE server.

```
execute interface pppoe-reconnect <interface>
```

Parameter	Description	Type	Size
<interface>	Reconnect PPPoE on this interface.	string	

execute internet-service4

internet-service4

This topic includes the following commands:

- [execute internet-service4 refresh on page 3637](#)

execute internet-service4 refresh

Refresh Internet Service Database(IPV4).

```
execute internet-service4 refresh
```

execute internet-service6

internet-service6

This topic includes the following commands:

- [execute internet-service6 refresh on page 3637](#)

execute internet-service6 refresh

Refresh Internet Service Database(IPV6).

```
execute internet-service6 refresh
```

execute ipam

ipam

This topic includes the following commands:

- [execute ipam create-dhcp-server on page 3637](#)

execute ipam create-dhcp-server

Create a DHCP server managed by IPAM.

```
execute ipam create-dhcp-server <interface>
```

Parameter	Description	Type	Size
<interface>	Interface for the DHCP server.	string	

execute iscsi

iscsi

This topic includes the following commands:

- [execute iscsi login on page 3638](#)
- [execute iscsi logout on page 3638](#)
- [execute iscsi show on page 3638](#)

execute iscsi login

Login to iSCSI.

```
execute iscsi login <name>
```

Parameter	Description	Type	Size
<name>	iSCSI name.	string	

execute iscsi logout

Logout from iSCSI.

```
execute iscsi logout <name>
```

Parameter	Description	Type	Size
<name>	iSCSI name.	string	

execute iscsi show

Show iSCSI info.

```
execute iscsi show <name>
```

Parameter	Description	Type	Size
<name>	iSCSI name.	string	

execute kmip

kmip

This topic includes the following commands:

- [execute kmip create on page 3639](#)
- [execute kmip destroy on page 3639](#)
- [execute kmip get on page 3640](#)
- [execute kmip locate on page 3640](#)
- [execute kmip rekey on page 3640](#)

execute kmip create

Create Symmetric key(s) in KMIP server

```
execute kmip create <kmip server> <algo> <keylen> <name>
```

Parameter	Description	Type	Size
<kmip server>	KMIP server name.	string	
<algo>	Cryptographic Algorithm.	string	
<keylen>	Key size (in bits).	string	
<name>	Key name (separate with ' ' or '*' for multiple items).	string	

execute kmip destroy

Destroy Symmetric key(s) in KMIP server

```
execute kmip destroy <kmip server> <keyid>
```

Parameter	Description	Type	Size
<kmip server>	KMIP server name.	string	
<keyid>	Key ID (in hex string, separate with ' ' or '*' for multiple items).	string	

execute kmip get

Get Symmetric key(s) from KMIP server

```
execute kmip get
```

execute kmip locate

locate Symmetric key(s) in KMIP server

```
execute kmip locate <kmip server> <name>
```

Parameter	Description	Type	Size
<kmip server>	KMIP server name.	string	
<name>	Key name (separate with ' ' or '*' for multiple items).	string	

execute kmip rekey

Rekey Symmetric key(s) from KMIP server

```
execute kmip rekey <kmip server> <keyid>
```

Parameter	Description	Type	Size
<kmip server>	KMIP server name.	string	
<keyid>	Key ID (in hex string, separate with ' ' or '*' for multiple items).	string	

execute log

log

This topic includes the following commands:

- [execute log backup ftp on page 3641](#)
- [execute log backup local on page 3642](#)
- [execute log backup tftp on page 3642](#)
- [execute log chroot on page 3642](#)
- [execute log delete on page 3642](#)
- [execute log delete-all on page 3643](#)

- [execute log detail on page 3643](#)
- [execute log display on page 3643](#)
- [execute log filter category on page 3643](#)
- [execute log filter device on page 3643](#)
- [execute log filter dump on page 3644](#)
- [execute log filter field on page 3644](#)
- [execute log filter free-style on page 3644](#)
- [execute log filter ha-member on page 3645](#)
- [execute log filter local-search-mode on page 3645](#)
- [execute log filter max-checklines on page 3645](#)
- [execute log filter pre-fetch-pages on page 3645](#)
- [execute log filter reset on page 3645](#)
- [execute log filter start-line on page 3646](#)
- [execute log filter view-lines on page 3646](#)
- [execute log flush-cache on page 3646](#)
- [execute log flush-cache-all on page 3646](#)
- [execute log fortianalyzer manual-failover on page 3646](#)
- [execute log fortianalyzer test-connectivity on page 3647](#)
- [execute log fortianalyzer-cloud test-connectivity on page 3647](#)
- [execute log fortianalyzer2 manual-failover on page 3647](#)
- [execute log fortianalyzer3 manual-failover on page 3647](#)
- [execute log fortiguard test-connectivity on page 3647](#)
- [execute log list on page 3647](#)
- [execute log raw-backup ftp on page 3648](#)
- [execute log raw-backup tftp on page 3648](#)
- [execute log restore on page 3648](#)
- [execute log roll on page 3649](#)
- [execute log shift-time on page 3649](#)
- [execute log upload on page 3649](#)
- [execute log upload-progress on page 3649](#)

execute log backup ftp

Backup logs and report databases to remote FTP server.

```
execute log backup ftp <filename> <ftp server>[:ftp port] <user> <passwd>
```

Parameter	Description	Type	Size
<filename>	Make file name on the remote FTP server	string	
<ftp server> [:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	

Parameter	Description	Type	Size
<user>	FTP username.	string	
<passwd>	FTP password.	string	

execute log backup local

Backup logs and report databases to local storage device.

```
execute log backup local <path>
```

Parameter	Description	Type	Size
<path>	Path to store logs and report databases.	string	

execute log backup tftp

Backup logs and report databases to remote TFTP server.

```
execute log backup tftp <filename> <tftp server>
```

Parameter	Description	Type	Size
<filename>	Make file name on the remote TFTP server	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute log chroot

Drop/Gain CLI root privilege.

```
execute log chroot
```

execute log delete

Delete local logs of one category.

```
execute log delete
```

execute log delete-all

Delete all local logs and recreate report database.

```
execute log delete-all
```

execute log detail

Display utm log entries for a particular traffic log.

```
execute log detail <category> <utmref>
```

Parameter	Description	Type	Size
<category>	Category for UTM logs	string	
<utmref>	You can copy and paste it from log display result by tuning on it using 'exec log filter show-utm-ref 1'	string	

execute log display

Display filtered log entries.

```
execute log display
```

execute log filter category

Category.

```
execute log filter category <category>
```

Parameter	Description	Type	Size
<category>	Category name, press enter for options.	string	

execute log filter device

Device to get log from.

```
execute log filter device <device>
```

Parameter	Description	Type	Size
<device>	Device name, press enter for options.	string	

execute log filter dump

Dump current filter settings.

```
execute log filter dump
```

execute log filter field

Filter by field.

```
execute log filter field <name> <argument 1> <argument 2> <argument 3> <argument 4> <argument 5>  
<argument 6> <argument 7>
```

Parameter	Description	Type	Size
<name>	Field name, press enter for options.	string	
<argument 1>	Field search argument 1, press enter for more help.	string	
<argument 2>	<argument 2>	string	
<argument 3>	<argument 3>	string	
<argument 4>	<argument 4>	string	
<argument 5>	<argument 5>	string	
<argument 6>	<argument 6>	string	
<argument 7>	<argument 7>	string	

execute log filter free-style

Filter by free-style expression.

```
execute log filter free-style <expression>
```

Parameter	Description	Type	Size
<expression>	Log filter expression.	string	

execute log filter ha-member

HA member.

```
execute log filter ha-member <sn>
```

Parameter	Description	Type	Size
<sn>	Serial number of HA member.	string	

execute log filter local-search-mode

local log search mode

```
execute log filter local-search-mode <mode>
```

Parameter	Description	Type	Size
<mode>	Local log search mode, press enter for options.	string	

execute log filter max-checklines

Maximum number of lines to check.

```
execute log filter max-checklines <number>
```

Parameter	Description	Type	Size
<number>	0 or (100 - 1000000).	string	

execute log filter pre-fetch-pages

Number of pages to check in advance under on-demand log search mode.

```
execute log filter pre-fetch-pages <number>
```

Parameter	Description	Type	Size
<number>	(2 - 10).	string	

execute log filter reset

Reset filter.

```
execute log filter reset <enter|all|field>
```

Parameter	Description	Type	Size
<enter all field>	<enter all> to reset all, <field> to reset field only.	string	

execute log filter start-line

Start line to display.

```
execute log filter start-line <number>
```

Parameter	Description	Type	Size
<number>	>=1	string	

execute log filter view-lines

Lines per view.

```
execute log filter view-lines <number>
```

Parameter	Description	Type	Size
<number>	Number of lines to view (5 - 1000).	string	

execute log flush-cache

Write disk log cache of current category to disk in compressed format.

```
execute log flush-cache
```

execute log flush-cache-all

Write disk log cache of all categories to disk in compressed format.

```
execute log flush-cache-all
```

execute log fortianalyzer manual-failover

Manually failover to use the other server.

```
execute log fortianalyzer manual-failover
```

execute log fortianalyzer test-connectivity

Query FortiAnalyzer connection status.

```
execute log fortianalyzer test-connectivity
```

execute log fortianalyzer-cloud test-connectivity

Query FortiAnalyzer Cloud connection status.

```
execute log fortianalyzer-cloud test-connectivity
```

execute log fortianalyzer2 manual-failover

Manually failover to use the other server.

```
execute log fortianalyzer2 manual-failover
```

execute log fortianalyzer3 manual-failover

Manually failover to use the other server.

```
execute log fortianalyzer3 manual-failover
```

execute log fortiguard test-connectivity

Query FortiGuard connection status.

```
execute log fortiguard test-connectivity
```

execute log list

List current and rolled log files info.

```
execute log list <category>
```

Parameter	Description	Type	Size
<category>	Category name, press enter for options.	string	

execute log raw-backup ftp

Backup raw logs to remote FTP server.

```
execute log raw-backup ftp <remotedir> <ftp server>[:ftp port] <user> <passwd>
```

Parameter	Description	Type	Size
<remotedir>	Remote directory on FTP server	string	
<ftp server> [:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<user>	FTP username.	string	
<passwd>	FTP password.	string	

execute log raw-backup tftp

Backup raw logs to remote TFTP server.

```
execute log raw-backup tftp <remotedir> <tftp server>
```

Parameter	Description	Type	Size
<remotedir>	Existing remote directory on TFTP server	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute log restore

Restore logs and report databases from local storage device.

```
execute log restore <path>
```

Parameter	Description	Type	Size
<path>	Path to restore logs and report databases.	string	

execute log roll

Roll log files now.

```
execute log roll
```

execute log shift-time

Shift log time stamps.

```
execute log shift-time <hours>
```

Parameter	Description	Type	Size
<hours>	Hours to shift log and report time stamps by.	string	

execute log upload

Upload log and archives to FortiAnalyzer/FortiCloud.

```
execute log upload
```

execute log upload-progress

Check FortiCloud upload progress.

```
execute log upload-progress
```

execute mem

mem

This topic includes the following commands:

- [execute mem add on page 3649](#)

execute mem add

Online new memory blocks.

```
execute mem add
```

execute mrouter

mrouter

This topic includes the following commands:

- [execute mrouter clear dense-routes on page 3650](#)
- [execute mrouter clear igmp-group on page 3650](#)
- [execute mrouter clear igmp-interface on page 3651](#)
- [execute mrouter clear multicast-routes on page 3651](#)
- [execute mrouter clear sparse-mode-bsr on page 3651](#)
- [execute mrouter clear sparse-routes on page 3651](#)
- [execute mrouter clear statistics on page 3652](#)

execute mrouter clear dense-routes

Clear PIM dense mode routes.

```
execute mrouter clear dense-routes <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Group IP address.	string	
<xxx.xxx.xxx.xxx>	Source IP address.	string	

execute mrouter clear igmp-group

Clear all IGMP entries for one or all groups.

```
execute mrouter clear igmp-group <xxx.xxx.xxx.xxx> <string>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Group IP address.	string	
<string>	Interface name.	string	

execute mrouter clear igmp-interface

Clear all IGMP entries from one interface.

```
execute mrouter clear igmp-interface <string>
```

Parameter	Description	Type	Size
<string>	Interface name.	string	

execute mrouter clear multicast-routes

Clear all PIM dense mode and sparse mode routes.

```
execute mrouter clear multicast-routes <xxx.xxx.xxx.xxx>|<0-511> <xxx.xxx.xxx.xxx>|<0-511> <0-511>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx> <0-511>	Group IP address or VRF ID.	string	
<xxx.xxx.xxx.xxx> <0-511>	Source IP address or VRF ID.	string	
<0-511>	VRF ID.	string	

execute mrouter clear sparse-mode-bsr

Clear PIM-SM RP sets learned from the BSR.

```
execute mrouter clear sparse-mode-bsr <0-511>
```

Parameter	Description	Type	Size
<0-511>	VRF ID.	string	

execute mrouter clear sparse-routes

Clear PIM sparse mode routes.

```
execute mrouter clear sparse-routes <xxx.xxx.xxx.xxx>|<0-511> <xxx.xxx.xxx.xxx>|<0-511> <0-511>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx> <0-511>	Group IP address or VRF ID.	string	

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx> <0-511>	Source IP address or VRF ID.	string	
<0-511>	VRF ID.	string	

execute mrouter clear statistics

Clear PIM routing statistics.

```
execute mrouter clear statistics <xxx.xxx.xxx.xxx>|<0-511> <xxx.xxx.xxx.xxx>|<0-511> <0-511>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx> <0-511>	Group IP address or VRF ID.	string	
<xxx.xxx.xxx.xxx> <0-511>	Source IP address or VRF ID.	string	
<0-511>	VRF ID.	string	

execute mrouter6

mrouter6

This topic includes the following commands:

- [execute mrouter6 clear mld on page 3652](#)
- [execute mrouter6 clear sparse-routes on page 3652](#)

execute mrouter6 clear mld

Clear PIM6 MLD group cache entries.

```
execute mrouter6 clear mld <X:X::X:X> <string>
```

Parameter	Description	Type	Size
<X:X::X:X>	Group IPv6 address.	string	
<string>	Interface name.	string	

execute mrouter6 clear sparse-routes

Clear PIM6 sparse mode routes.

```
execute mrouter6 clear sparse-routes <X:X::X:X> <X:X::X:X>
```

Parameter	Description	Type	Size
<X:X::X:X>	Group IPv6 address.	string	
<X:X::X:X>	Source IPv6 address.	string	

execute nsx

nsx

This topic includes the following commands:

- [execute nsx group delete on page 3653](#)
- [execute nsx group import on page 3653](#)
- [execute nsx group list on page 3654](#)

execute nsx group delete

Delete NSX Security Groups.

```
execute nsx group delete <vdom> <filter>
```

Parameter	Description	Type	Size
<vdom>	VDOM.	string	
<filter>	Name Filter.	string	

execute nsx group import

Import NSX Security Groups.

```
execute nsx group import <name> <vdom> <filter>
```

Parameter	Description	Type	Size
<name>	SDN connector.	string	
<vdom>	VDOM.	string	
<filter>	Name Filter.	string	

execute nsx group list

List NSX Security Groups.

```
execute nsx group list <name> <filter>
```

Parameter	Description	Type	Size
<name>	SDN connector.	string	
<filter>	Name Filter.	string	

execute oqs

OQS command to see available PQC KEM algorithms and generate test data.

```
execute oqs
```

execute ping

PING command.

```
execute ping <ip>
```

Parameter	Description	Type	Size
<ip>	IP address or domain name.	string	

execute ping6

PINGv6 command.

```
execute ping6
```

execute ping6-options

ping6-options

This topic includes the following commands:

- [execute ping6-options adaptive-ping on page 3655](#)
- [execute ping6-options data-size on page 3655](#)
- [execute ping6-options interface on page 3656](#)
- [execute ping6-options interval on page 3656](#)
- [execute ping6-options pattern on page 3656](#)
- [execute ping6-options repeat-count on page 3656](#)
- [execute ping6-options reset on page 3656](#)
- [execute ping6-options source6 on page 3657](#)
- [execute ping6-options timeout on page 3657](#)
- [execute ping6-options tos on page 3657](#)
- [execute ping6-options ttl on page 3657](#)
- [execute ping6-options use-sdwan on page 3658](#)
- [execute ping6-options validate-reply on page 3658](#)
- [execute ping6-options view-settings on page 3658](#)
- [execute ping6-options vrf on page 3658](#)

execute ping6-options adaptive-ping

Adaptive ping <enable|disable>.

```
execute ping6-options adaptive-ping <string>
```

Parameter	Description	Type	Size
<string>	<enable disable>.	string	

execute ping6-options data-size

Integer value to specify datagram size in bytes.

```
execute ping6-options data-size <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [0,65507].	string	

execute ping6-options interface

Auto | <outgoing interface>.

```
execute ping6-options interface <string>
```

Parameter	Description	Type	Size
<string>	Auto <outgoing interface>.	string	

execute ping6-options interval

Integer value to specify seconds to wait between two pings.

```
execute ping6-options interval <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [1, 2147483647]	string	

execute ping6-options pattern

Hex format of pattern, e.g. 00ffaabb.

```
execute ping6-options pattern <string>
```

Parameter	Description	Type	Size
<string>	Hex format of pattern, e.g. 00ffaabb.	string	

execute ping6-options repeat-count

Integer value to specify how many times to repeat PING.

```
execute ping6-options repeat-count <string>
```

Parameter	Description	Type	Size
<string>	Integer value [1, 2147483647]	string	

execute ping6-options reset

Reset settings.


```
execute ping6-options reset
```

execute ping6-options source6

Auto | <source interface IPv6>.

```
execute ping6-options source6 <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>
```

Parameter	Description	Type	Size
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>	<source interface IPv6> Auto	string	

execute ping6-options timeout

Integer value to specify timeout in seconds.

```
execute ping6-options timeout <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [0, 2147483647]	string	

execute ping6-options tos

IPv6 type-of-service (traffic class) value.

```
execute ping6-options tos <integer>
```

Parameter	Description	Type	Size
<integer>	Hex number [0x00, 0xFF]	string	

execute ping6-options ttl

Integer value to specify time-to-live.

```
execute ping6-options ttl <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [1,255]	string	

execute ping6-options use-sdwan

Use SD-WAN rules to get output interface <yes | no>.

```
execute ping6-options use-sdwan <string>
```

Parameter	Description	Type	Size
<string>	<yes no>.	string	

execute ping6-options validate-reply

Validate reply data <yes | no>.

```
execute ping6-options validate-reply <string>
```

Parameter	Description	Type	Size
<string>	<yes no>.	string	

execute ping6-options view-settings

View the current settings for PING option.

```
execute ping6-options view-settings
```

execute ping6-options vrf

VRF ID.

```
execute ping6-options vrf <integer>
```

Parameter	Description	Type	Size
<integer>	<0-511>	string	

execute ping-options

ping-options

This topic includes the following commands:

- [execute ping-options adaptive-ping on page 3659](#)
- [execute ping-options data-size on page 3659](#)
- [execute ping-options df-bit on page 3659](#)
- [execute ping-options interface on page 3660](#)
- [execute ping-options interval on page 3660](#)
- [execute ping-options pattern on page 3660](#)
- [execute ping-options repeat-count on page 3660](#)
- [execute ping-options reset on page 3661](#)
- [execute ping-options source on page 3661](#)
- [execute ping-options timeout on page 3661](#)
- [execute ping-options tos on page 3661](#)
- [execute ping-options ttl on page 3661](#)
- [execute ping-options use-sdwan on page 3662](#)
- [execute ping-options validate-reply on page 3662](#)
- [execute ping-options view-settings on page 3662](#)
- [execute ping-options vrf on page 3662](#)

execute ping-options adaptive-ping

Adaptive ping <enable|disable>.

```
execute ping-options adaptive-ping <string>
```

Parameter	Description	Type	Size
<string>	<enable disable>.	string	

execute ping-options data-size

Integer value to specify datagram size in bytes.

```
execute ping-options data-size <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [0,65507].	string	

execute ping-options df-bit

Set DF bit in IP header <yes | no>.

```
execute ping-options df-bit <string>
```

Parameter	Description	Type	Size
<string>	<yes no>.	string	

execute ping-options interface

Auto | <outgoing interface>.

```
execute ping-options interface <string>
```

Parameter	Description	Type	Size
<string>	Auto <outgoing interface>.	string	

execute ping-options interval

Integer value to specify seconds between two pings.

```
execute ping-options interval <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [1, 2147483647]	string	

execute ping-options pattern

Hex format of pattern, e.g. 00ffaabb.

```
execute ping-options pattern <string>
```

Parameter	Description	Type	Size
<string>	Hex format of pattern, e.g. 00ffaabb.	string	

execute ping-options repeat-count

Integer value to specify how many times to repeat PING.

```
execute ping-options repeat-count <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [1, 2147483647]	string	

execute ping-options reset

Reset settings.

```
execute ping-options reset
```

execute ping-options source

Auto | <source interface IP>.

```
execute ping-options source <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	<source interface IP> Auto	string	

execute ping-options timeout

Integer value to specify timeout in seconds.

```
execute ping-options timeout <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [0, 2147483647]	string	

execute ping-options tos

IP type-of-service option.

```
execute ping-options tos <string>
```

Parameter	Description	Type	Size
<string>	default IP TOS defaults to 0 lowcost IP TOS minimize cost lowdelay IP TOS minimize delay reliability IP TOS maximize reliability throughput IP TOS maximize throughput	string	

execute ping-options ttl

Integer value to specify time-to-live.

```
execute ping-options ttl <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [1,255].	string	

execute ping-options use-sdwan

Use SD-WAN rules to get output interface <yes | no>.

```
execute ping-options use-sdwan <string>
```

Parameter	Description	Type	Size
<string>	<yes no>.	string	

execute ping-options validate-reply

Validate reply data <yes | no>.

```
execute ping-options validate-reply <string>
```

Parameter	Description	Type	Size
<string>	<yes no>.	string	

execute ping-options view-settings

View the current settings for PING option.

```
execute ping-options view-settings
```

execute ping-options vrf

VRF ID.

```
execute ping-options vrf <integer>
```

Parameter	Description	Type	Size
<integer>	<0-511>	string	

execute policy-packet-capture

policy-packet-capture

This topic includes the following commands:

- [execute policy-packet-capture delete-all on page 3663](#)

execute policy-packet-capture delete-all

Delete all captured packet.

```
execute policy-packet-capture delete-all
```

execute reboot

Reboot now.

```
execute reboot <comment> <string>
```

Parameter	Description	Type	Size
<comment>	comment	string	
<string>	Reboot comments.	string	

execute replace-device

replace-device

This topic includes the following commands:

- [execute replace-device fortiap on page 3663](#)
- [execute replace-device fortiswitch on page 3664](#)

execute replace-device fortiap

FortiAP.

```
execute replace-device fortiap <fortiap-id> <fortiap-id>
```

Parameter	Description	Type	Size
<fortiap-id>	Old FortiAP serial number.	string	
<fortiap-id>	New FortiAP serial number.	string	

execute replace-device fortiswitch

FortiSwitch.

```
execute replace-device fortiswitch <fortiswitch-id> <fortiswitch-id>
```

Parameter	Description	Type	Size
<fortiswitch-id>	Existing FortiSwitch serial number.	string	
<fortiswitch-id>	New FortiSwitch serial number.	string	

execute report

report

This topic includes the following commands:

- [execute report flush-cache on page 3664](#)
- [execute report recreate-db on page 3664](#)
- [execute report run on page 3665](#)
- [execute report sandbox-status on page 3665](#)

execute report flush-cache

Flush report caches

```
execute report flush-cache
```

execute report recreate-db

Recreate the report database

```
execute report recreate-db
```


execute report run

generate a report, only last 7-days data available

```
execute report run [layout name] [Start Time] [End Time]
```

Parameter	Description	Type	Size
[layout name]	Layout name for a report. If not provided, the default layout will be used.	string	
[Start Time]	Start time of the report time period ("yyyy-mm-dd hh").	string	
[End Time]	End time of the report time period ("yyyy-mm-dd hh").	string	

execute report sandbox-status

sending sandbox status for testing

```
execute report sandbox-status [status] [sha256]
```

Parameter	Description	Type	Size
[status]	The status of sandbox returning result	string	
[sha256]	SHA256 checksum	string	

execute report-config

report-config

This topic includes the following commands:

- [execute report-config reset on page 3665](#)

execute report-config reset

Reset report templates to the factory default

```
execute report-config reset
```

execute restore

restore

This topic includes the following commands:

- [execute restore av ftp on page 3666](#)
- [execute restore av tftp on page 3667](#)
- [execute restore config dhcp on page 3667](#)
- [execute restore config flash on page 3667](#)
- [execute restore config ftp on page 3668](#)
- [execute restore config management-station normal on page 3668](#)
- [execute restore config management-station script on page 3668](#)
- [execute restore config management-station template on page 3668](#)
- [execute restore config tftp on page 3669](#)
- [execute restore image flash on page 3669](#)
- [execute restore image ftp on page 3669](#)
- [execute restore image management-station on page 3670](#)
- [execute restore image tftp on page 3670](#)
- [execute restore image url on page 3670](#)
- [execute restore ips ftp on page 3670](#)
- [execute restore ips tftp on page 3671](#)
- [execute restore ipsuserdefsig ftp on page 3671](#)
- [execute restore ipsuserdefsig tftp on page 3671](#)
- [execute restore manual-license ftp on page 3672](#)
- [execute restore manual-license tftp on page 3672](#)
- [execute restore other-objects ftp on page 3672](#)
- [execute restore other-objects tftp on page 3673](#)
- [execute restore script ftp on page 3673](#)
- [execute restore script lastlog on page 3673](#)
- [execute restore script scp on page 3674](#)
- [execute restore script tftp on page 3674](#)
- [execute restore vmlicense ftp on page 3674](#)
- [execute restore vmlicense tftp on page 3675](#)

execute restore av ftp

Restore antivirus database from FTP server.

```
execute restore av ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	Antivirus data base file name (path) on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute restore av tftp

Restore antivirus database from TFTP server.

```
execute restore av tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	Antivirus database file name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute restore config dhcp

Load config file via DHCP.

```
execute restore config dhcp <port> <Enter> | <vlanid>
```

Parameter	Description	Type	Size
<port>	Port to be DHCP client.	string	
<Enter> <vlanid>	Enter or specify VLAN ID to create a VLAN on the <port>.	string	

execute restore config flash

Load config file from flash to firewall.

```
execute restore config flash <revision>
```

Parameter	Description	Type	Size
<revision>	Revision ID on the flash.	string	

execute restore config ftp

Load config file from FTP server.

```
execute restore config ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>  
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Configure file name(path) on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter> <passwd>	Password may be needed to restore.	string	

execute restore config management-station normal

Load normal config file from management station to firewall.

```
execute restore config management-station normal <revision>
```

Parameter	Description	Type	Size
<revision>	Revision to retrieve, or enter '0' to get latest revision list.	string	

execute restore config management-station script

Load script config file from management station to firewall.

```
execute restore config management-station script <revision>
```

Parameter	Description	Type	Size
<revision>	Revision to retrieve, or enter '0' to get latest revision list.	string	

execute restore config management-station template

Load template config file from management station to firewall.

```
execute restore config management-station template <revision>
```

Parameter	Description	Type	Size
<revision>	Revision to retrieve, or enter '0' to get latest revision list.	string	

execute restore config tftp

Load config file from TFTP server to firewall.

```
execute restore config tftp <string> <tftp server> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter> <passwd>	Password may be needed to restore.	string	

execute restore image flash

Restore image from flash.

```
execute restore image flash <revision>
```

Parameter	Description	Type	Size
<revision>	Image revision ID on flash.	string	

execute restore image ftp

Load image from FTP server.

```
execute restore image ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	Image file name(path) on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute restore image management-station

Restore image from Management station.

```
execute restore image management-station <string>
```

Parameter	Description	Type	Size
<string>	Image ID on the server.	string	

execute restore image tftp

Restore image from TFTP server.

```
execute restore image tftp <string> <tftp address>
```

Parameter	Description	Type	Size
<string>	Image file name on the TFTP server.	string	
<tftp address>	TFTP server IPv4, IPv6, or FQDN.	string	

execute restore image url

Restore image from URL with HTTP/HTTPS protocols. Decrypt image if needed.

```
execute restore image url <string> <Enter>|<passwd>|<force> <Enter>|<force>
```

Parameter	Description	Type	Size
<string>	URL string with protocol prefix. e.g: https://example.com/image.aes	string	
<Enter> <passwd> <force>	Image encryption passphrase.	string	
<Enter> <force>	Bypass signature and validity checking.	string	

execute restore ips ftp

Restore IPS database from FTP server.

```
execute restore ips ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	IPS data base file name (path) on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute restore ips tftp

Restore IPS database from TFTP server.

```
execute restore ips tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	IPS database file name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute restore ipsuserdefsig ftp

Restore user-defined ips signatures file from FTP server.

```
execute restore ipsuserdefsig ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	User-defined ips signatures file on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute restore ipsuserdefsig tftp

Restore user defined IPS signatures file from TFTP server.

```
execute restore ipsuserdefsig tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute restore manual-license ftp

Restore Manual License from FTP server.

```
execute restore manual-license ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	FortiGuard Contract License file name on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute restore manual-license tftp

Restore Manual License from TFTP server.

```
execute restore manual-license tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	FortiGuard Contract License file name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute restore other-objects ftp

Restore other FortiGuard packages from FTP server. Current support: Internet-service Database Apps/Maps, URL Allow List, DLP signatures and CASB signatures.

```
execute restore other-objects ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	Other FortiGuard package file name on the FTP server.	string	

Parameter	Description	Type	Size
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute restore other-objects tftp

Restore other FortiGuard packages from TFTP server. Current support: Internet-service Database Apps/Maps, URL Allow List, DLP signatures and CASB signatures.

```
execute restore other-objects tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	Other FortiGuard package file name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute restore script ftp

Load script from FTP server.

```
execute restore script ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	Script on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute restore script lastlog

Read the result of last restored script.

```
execute restore script lastlog
```

execute restore script scp

Load script from SCP server to firewall.

```
execute restore script scp <string> <ip> <user> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	File name on the SCP server.	string	
<ip>	IP address.	string	
<user>	User name.	string	
<Enter> <passwd>	Enter or input password.	string	

execute restore script tftp

Load script from TFTP server to firewall.

```
execute restore script tftp <string> <tftp server> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter> <passwd>	Password may be needed to restore.	string	

execute restore vmlicense ftp

Restore VM license from FTP server.

```
execute restore vmlicense ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	VM license file name(path) on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute restore vmlicense tftp

restore VM license from tftp server

```
execute restore vmlicense tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	VM license file name on the tftp server	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute revision

revision

This topic includes the following commands:

- [execute revision delete config on page 3675](#)
- [execute revision delete image on page 3675](#)
- [execute revision list config on page 3676](#)
- [execute revision list image on page 3676](#)

execute revision delete config

Delete config revision on local disk.

```
execute revision delete config <revision> <rev_id>
```

Parameter	Description	Type	Size
<revision>	Revision ID(s) on local disk. Eg. 1 3-6 8	string	
<rev_id>	place holder for multiple Revision IDs, at most 10 a time.	string	

execute revision delete image

Delete image revision on local disk.

```
execute revision delete image <revision> <rev_id>
```

Parameter	Description	Type	Size
<revision>	Revision ID(s) on local disk. Eg. 1 3-6 8	string	
<rev_id>	place holder for multiple Revision IDs, at most 10 a time.	string	

execute revision list config

List config revision on local disk.

```
execute revision list config
```

execute revision list image

List image revision on local disk.

```
execute revision list image
```

execute router

router

This topic includes the following commands:

- [execute router clear bfd session on page 3676](#)
- [execute router clear bgp all on page 3677](#)
- [execute router clear bgp as on page 3677](#)
- [execute router clear bgp dampening on page 3677](#)
- [execute router clear bgp external on page 3677](#)
- [execute router clear bgp flap-statistics on page 3677](#)
- [execute router clear bgp group on page 3678](#)
- [execute router clear bgp ip on page 3678](#)
- [execute router clear bgp ipv6 on page 3678](#)
- [execute router clear ospf process on page 3678](#)
- [execute router clear ospf6 process on page 3678](#)
- [execute router restart on page 3678](#)

execute router clear bfd session

Clear BFD session.

```
execute router clear bfd session <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx> <string>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP address.	string	
<xxx.xxx.xxx.xxx>	Destination IP address.	string	
<string>	Interface name.	string	

execute router clear bgp all

Clear all BGP peers.

```
execute router clear bgp all
```

execute router clear bgp as

Clear BGP peer by AS number.

```
execute router clear bgp as
```

execute router clear bgp dampening

Clear route flap dampening information.

```
execute router clear bgp dampening
```

execute router clear bgp external

Clear all external peers.

```
execute router clear bgp external
```

execute router clear bgp flap-statistics

Clear route flap statistics.

```
execute router clear bgp flap-statistics
```

execute router clear bgp group

Clear BGP peer by group.

```
execute router clear bgp group
```

execute router clear bgp ip

Clear BGP peer by IP address.

```
execute router clear bgp ip
```

execute router clear bgp ipv6

Clear BGP peer by IPv6 address.

```
execute router clear bgp ipv6
```

execute router clear ospf process

Clear and restart OSPF router.

```
execute router clear ospf process
```

execute router clear ospf6 process

Clear and restart OSPF6 router.

```
execute router clear ospf6 process
```

execute router restart

Restart routing software.

```
execute router restart
```

execute sdn

sdn

This topic includes the following commands:

- [execute sdn tag add nsx on page 3679](#)
- [execute sdn tag remove nsx on page 3679](#)

execute sdn tag add nsx

NSX tag VM.

```
execute sdn tag add nsx <name> <ip-addr> <tagname> <0/1>
```

Parameter	Description	Type	Size
<name>	NSX SDN connector name.	string	
<ip-addr>	VM IP address.	string	
<tagname>	Tag name.	string	
<0/1>	Disable/enable use of Spoofguard.	string	

execute sdn tag remove nsx

NSX remove VM from tag.

```
execute sdn tag remove nsx <name> <ip-addr> <tagname> <0/1>
```

Parameter	Description	Type	Size
<name>	NSX SDN connector name.	string	
<ip-addr>	VM IP address.	string	
<tagname>	Tag name.	string	
<0/1>	Disable/enable use of Spoofguard.	string	

execute sdn-vpn

sdn-vpn

This topic includes the following commands:

- [execute sdn-vpn discover aws-tgw on page 3680](#)
- [execute sdn-vpn discover aws-vgw on page 3680](#)

execute sdn-vpn discover aws-tgw

Discover AWS virtual private gateways.

```
execute sdn-vpn discover aws-tgw <name>
```

Parameter	Description	Type	Size
<name>	SDN Connector name.	string	

execute sdn-vpn discover aws-vgw

Discover AWS virtual private gateways.

```
execute sdn-vpn discover aws-vgw <name>
```

Parameter	Description	Type	Size
<name>	SDN Connector name.	string	

execute send-fds-statistics

Send FortiGuard statistics.

```
execute send-fds-statistics
```

execute send-fmg-list

Send connected FortiManager list to FortiGuard.

```
execute send-fmg-list
```


execute set

set

This topic includes the following commands:

- [execute set system session filter clear all on page 3681](#)
- [execute set system session filter clear dport on page 3682](#)
- [execute set system session filter clear dst on page 3682](#)
- [execute set system session filter clear duration on page 3682](#)
- [execute set system session filter clear expire on page 3682](#)
- [execute set system session filter clear policy on page 3682](#)
- [execute set system session filter clear proto on page 3682](#)
- [execute set system session filter clear sport on page 3683](#)
- [execute set system session filter clear src on page 3683](#)
- [execute set system session filter clear vd on page 3683](#)
- [execute set system session filter dport on page 3683](#)
- [execute set system session filter dst on page 3683](#)
- [execute set system session filter duration on page 3684](#)
- [execute set system session filter expire on page 3684](#)
- [execute set system session filter list on page 3684](#)
- [execute set system session filter negate dport on page 3684](#)
- [execute set system session filter negate dst on page 3684](#)
- [execute set system session filter negate duration on page 3685](#)
- [execute set system session filter negate expire on page 3685](#)
- [execute set system session filter negate policy on page 3685](#)
- [execute set system session filter negate proto on page 3685](#)
- [execute set system session filter negate sport on page 3685](#)
- [execute set system session filter negate src on page 3685](#)
- [execute set system session filter negate vd on page 3686](#)
- [execute set system session filter policy on page 3686](#)
- [execute set system session filter proto on page 3686](#)
- [execute set system session filter sport on page 3686](#)
- [execute set system session filter src on page 3687](#)
- [execute set system session filter vd on page 3687](#)

execute set system session filter clear all

Clear session filter.

```
execute set system session filter clear all
```

execute set system session filter clear dport

Clear destination port.

```
execute set system session filter clear dport
```

execute set system session filter clear dst

Clear destination IP.

```
execute set system session filter clear dst
```

execute set system session filter clear duration

Clear duration.

```
execute set system session filter clear duration
```

execute set system session filter clear expire

Clear expire.

```
execute set system session filter clear expire
```

execute set system session filter clear policy

Clear policy ID.

```
execute set system session filter clear policy
```

execute set system session filter clear proto

Clear protocol.

```
execute set system session filter clear proto
```

execute set system session filter clear sport

Clear source port.

```
execute set system session filter clear sport
```

execute set system session filter clear src

Clear source IP.

```
execute set system session filter clear src
```

execute set system session filter clear vd

Clear virtual domain.

```
execute set system session filter clear vd
```

execute set system session filter dport

Destination port.

```
execute set system session filter dport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

execute set system session filter dst

Destination IP address.

```
execute set system session filter dst <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP (from).	string	
<xxx.xxx.xxx.xxx>	Destination IP (to).	string	

execute set system session filter duration

duration

```
execute set system session filter duration <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Duration (from).	string	
<xxx>	Duration (to).	string	

execute set system session filter expire

expire

```
execute set system session filter expire <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Expire (from).	string	
<xxx>	Expire (to).	string	

execute set system session filter list

List system session filter.

```
execute set system session filter list
```

execute set system session filter negate dport

Inverse destination port.

```
execute set system session filter negate dport
```

execute set system session filter negate dst

Inverse destination IP.

```
execute set system session filter negate dst
```

execute set system session filter negate duration

Inverse duration.

```
execute set system session filter negate duration
```

execute set system session filter negate expire

Inverse expire.

```
execute set system session filter negate expire
```

execute set system session filter negate policy

Inverse policy ID.

```
execute set system session filter negate policy
```

execute set system session filter negate proto

Inverse protocol.

```
execute set system session filter negate proto
```

execute set system session filter negate sport

Inverse source port.

```
execute set system session filter negate sport
```

execute set system session filter negate src

Inverse source IP.

```
execute set system session filter negate src
```

execute set system session filter negate vd

Inverse virtual domain.

```
execute set system session filter negate vd
```

execute set system session filter policy

Policy ID.

```
execute set system session filter policy <xxx> <xxx>
```

Parameter	Description	Type	Size
<xxx>	Policy ID (from).	string	
<xxx>	Policy ID (to).	string	

execute set system session filter proto

Protocol number.

```
execute set system session filter proto <xx> <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255> (from).	string	
<xx>	<0-255> (to).	string	

execute set system session filter sport

Source port.

```
execute set system session filter sport <xxxx> <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	
<xxxx>	<0-65535> (to).	string	

execute set system session filter src

Source IP address.

```
execute set system session filter src <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (from).	string	
<xxx.xxx.xxx.xxx>	Source IP (to).	string	

execute set system session filter vd

Index of virtual domain. -1 matches all.

```
execute set system session filter vd <xxx>
```

Parameter	Description	Type	Size
<xxx>	Index of virtual domain. -1 matches all.	string	

execute shutdown

Shutdown now.

```
execute shutdown <comment> <string>
```

Parameter	Description	Type	Size
<comment>	comment	string	
<string>	Shutdown comments.	string	

execute speed-test

A bandwidth measuring tool.

```
execute speed-test <interface> <server> <mode>
```

Parameter	Description	Type	Size
<interface>	auto <outgoing interface name>.	string	
<server>	server name.	string	
<mode>	optional, Auto(default), TCP or UDP.	string	

execute speed-test-custom

Run speed test to a custom server.

```
execute speed-test-custom <interface> <server>
```

Parameter	Description	Type	Size
<interface>	Speed test interface.	string	
<server>	Server address.	string	

execute speed-test-ipsec

Measure the bandwidth of the underlay of a IPSec tunnel.

```
execute speed-test-ipsec <interface> <tunnel_name>
```

Parameter	Description	Type	Size
<interface>	ipsec phase1 interface.	string	
<tunnel_name>	all <specific tunnel name>.	string	

execute speed-test-options

speed-test-options

This topic includes the following commands:

- [execute speed-test-options blksize on page 3689](#)
- [execute speed-test-options burst on page 3689](#)
- [execute speed-test-options ctrl-port on page 3689](#)

- [execute speed-test-options duration on page 3690](#)
- [execute speed-test-options get-token on page 3690](#)
- [execute speed-test-options max-down on page 3690](#)
- [execute speed-test-options max-up on page 3690](#)
- [execute speed-test-options protocol on page 3691](#)
- [execute speed-test-options reset on page 3691](#)
- [execute speed-test-options reset-token on page 3691](#)
- [execute speed-test-options server-port on page 3691](#)
- [execute speed-test-options set-shaper on page 3691](#)
- [execute speed-test-options show on page 3692](#)
- [execute speed-test-options tos on page 3692](#)

execute speed-test-options blksize

Set blksize.

```
execute speed-test-options blksize <blksize>
```

Parameter	Description	Type	Size
<blksize>	0-2147483647	string	

execute speed-test-options burst

Set number of burst packet in UDP test.

```
execute speed-test-options burst <burst>
```

Parameter	Description	Type	Size
<burst>	0-2147483647	string	

execute speed-test-options ctrl-port

Set test controller port.

```
execute speed-test-options ctrl-port <port>
```

Parameter	Description	Type	Size
<port>	0-65535	string	

execute speed-test-options duration

Set test duration in seconds.

```
execute speed-test-options duration <duration>
```

Parameter	Description	Type	Size
<duration>	5-2147483647	string	

execute speed-test-options get-token

Obtain test token via ipsec tunnel.

```
execute speed-test-options get-token <ipsec-p1-name> <tunnel>
```

Parameter	Description	Type	Size
<ipsec-p1-name>	IPSec phase1 interface.	string	
<tunnel>	tunnel name.	string	

execute speed-test-options max-down

Set maximum downloading rate (kbps).

```
execute speed-test-options max-down <max-down>
```

Parameter	Description	Type	Size
<max-down>	0-2147483647	string	

execute speed-test-options max-up

Set maximum uploading rate (kbps).

```
execute speed-test-options max-up <max-up>
```

Parameter	Description	Type	Size
<max-up>	0-2147483647	string	

execute speed-test-options protocol

Set protocol.

```
execute speed-test-options protocol <protocol>
```

Parameter	Description	Type	Size
<protocol>	TCP or UDP	string	

execute speed-test-options reset

Reset options to default.

```
execute speed-test-options reset
```

execute speed-test-options reset-token

Reset saved token.

```
execute speed-test-options reset-token
```

execute speed-test-options server-port

Set test server port.

```
execute speed-test-options server-port <port>
```

Parameter	Description	Type	Size
<port>	0-65535	string	

execute speed-test-options set-shaper

Notify server to set egress shaper based on test results.

```
execute speed-test-options set-shaper <enable | disable>
```

Parameter	Description	Type	Size
<enable disable>	<enable disable>	string	

execute speed-test-options show

Show options.

```
execute speed-test-options show
```

execute speed-test-options tos

Set TOS.

```
execute speed-test-options tos <tos>
```

Parameter	Description	Type	Size
<tos>	TOS	string	

execute speed-test-server

speed-test-server

This topic includes the following commands:

- [execute speed-test-server download on page 3692](#)
- [execute speed-test-server list on page 3692](#)

execute speed-test-server download

Download server list from FortiGate Cloud.

```
execute speed-test-server download
```

execute speed-test-server list

List all available servers.

```
execute speed-test-server list
```

execute ssh

Simple SSH client.

```
execute ssh <user@host> <port>
```

Parameter	Description	Type	Size
<user@host>	User-name @ IP address or domain name.	string	
<port>	port.	string	

execute ssh6

Simple IPv6 SSH client.

```
execute ssh6 <user@host> <port>
```

Parameter	Description	Type	Size
<user@host>	User-name @ IPv6 address or domain name.	string	
<port>	port.	string	

execute ssh6-options

ssh6-options

This topic includes the following commands:

- [execute ssh6-options interface on page 3693](#)
- [execute ssh6-options reset on page 3694](#)
- [execute ssh6-options source6 on page 3694](#)
- [execute ssh6-options view-settings on page 3694](#)

execute ssh6-options interface

Auto | <outgoing interface>.

```
execute ssh6-options interface <string>
```

Parameter	Description	Type	Size
<string>	Auto <outgoing interface>.	string	

execute ssh6-options reset

Reset settings.

```
execute ssh6-options reset
```

execute ssh6-options source6

Auto | <source interface IPv6>.

```
execute ssh6-options source6 <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>
```

Parameter	Description	Type	Size
<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>	<source interface IPv6> Auto	string	

execute ssh6-options view-settings

View current settings for SSH (IPv6) option.

```
execute ssh6-options view-settings
```

execute ssh-options

ssh-options

This topic includes the following commands:

- [execute ssh-options interface on page 3694](#)
- [execute ssh-options reset on page 3695](#)
- [execute ssh-options source on page 3695](#)
- [execute ssh-options view-settings on page 3695](#)

execute ssh-options interface

Auto | <outgoing interface>.

```
execute ssh-options interface <string>
```

Parameter	Description	Type	Size
<string>	Auto <outgoing interface>.	string	

execute ssh-options reset

Reset settings.

```
execute ssh-options reset
```

execute ssh-options source

Auto | <source interface IP>.

```
execute ssh-options source <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	<source interface IP> Auto	string	

execute ssh-options view-settings

View the current settings for SSH option.

```
execute ssh-options view-settings
```

execute ssh-regen-keys

Regenerate SSH server keys.

```
execute ssh-regen-keys
```

execute switch-controller

switch-controller

This topic includes the following commands:

- [execute switch-controller custom-command on page 3697](#)
- [execute switch-controller diagnose-connection on page 3697](#)
- [execute switch-controller diagnose-connection-v6 on page 3698](#)
- [execute switch-controller flapguard reset on page 3698](#)
- [execute switch-controller get-conn-status on page 3698](#)
- [execute switch-controller get-physical-conn dot on page 3698](#)
- [execute switch-controller get-physical-conn standard on page 3699](#)
- [execute switch-controller get-sync-status all on page 3699](#)
- [execute switch-controller get-sync-status group on page 3699](#)
- [execute switch-controller get-sync-status serial on page 3699](#)
- [execute switch-controller get-sync-status switch-id on page 3700](#)
- [execute switch-controller get-upgrade-status on page 3700](#)
- [execute switch-controller ssh on page 3700](#)
- [execute switch-controller switch-action 802-1X clear-auth-mac on page 3700](#)
- [execute switch-controller switch-action 802-1X clear-auth-port on page 3701](#)
- [execute switch-controller switch-action bpdu-guard reset on page 3701](#)
- [execute switch-controller switch-action cable-diag on page 3701](#)
- [execute switch-controller switch-action factory-reset on page 3701](#)
- [execute switch-controller switch-action flow-tracking delete-flows-all on page 3702](#)
- [execute switch-controller switch-action flow-tracking expire-flows-all on page 3702](#)
- [execute switch-controller switch-action igmp-snoop clear-learned on page 3702](#)
- [execute switch-controller switch-action loop-guard reset on page 3702](#)
- [execute switch-controller switch-action mac-device-reset dynamic on page 3703](#)
- [execute switch-controller switch-action mac-device-reset nac on page 3703](#)
- [execute switch-controller switch-action mac-limit-violation reset all on page 3703](#)
- [execute switch-controller switch-action mac-limit-violation reset interface on page 3704](#)
- [execute switch-controller switch-action mac-limit-violation reset vlan on page 3704](#)
- [execute switch-controller switch-action mclag stats clear icl on page 3704](#)
- [execute switch-controller switch-action mclag stats clear mlag on page 3704](#)
- [execute switch-controller switch-action physical-ports led-flash switch-group on page 3705](#)
- [execute switch-controller switch-action physical-ports led-flash switch-id on page 3705](#)
- [execute switch-controller switch-action physical-ports led-flash tier1 on page 3705](#)
- [execute switch-controller switch-action physical-ports led-flash tier2plus on page 3706](#)
- [execute switch-controller switch-action poe reset on page 3706](#)
- [execute switch-controller switch-action restart delay all on page 3706](#)
- [execute switch-controller switch-action restart delay switch-group on page 3706](#)
- [execute switch-controller switch-action restart delay switch-id on page 3707](#)
- [execute switch-controller switch-action restart swtp all on page 3707](#)
- [execute switch-controller switch-action restart swtp switch-group on page 3707](#)
- [execute switch-controller switch-action restart swtp switch-id on page 3707](#)
- [execute switch-controller switch-action set-standalone on page 3708](#)

- [execute switch-controller switch-action sticky-mac delete-unsaved all on page 3708](#)
- [execute switch-controller switch-action sticky-mac delete-unsaved interface on page 3708](#)
- [execute switch-controller switch-action sticky-mac save all on page 3709](#)
- [execute switch-controller switch-action sticky-mac save interface on page 3709](#)
- [execute switch-controller switch-software cancel all on page 3709](#)
- [execute switch-controller switch-software cancel switch-group on page 3709](#)
- [execute switch-controller switch-software cancel switch-id on page 3710](#)
- [execute switch-controller switch-software delete on page 3710](#)
- [execute switch-controller switch-software list-available on page 3710](#)
- [execute switch-controller switch-software stage all on page 3710](#)
- [execute switch-controller switch-software stage switch-group on page 3710](#)
- [execute switch-controller switch-software stage switch-id on page 3711](#)
- [execute switch-controller switch-software upgrade on page 3711](#)
- [execute switch-controller switch-software upload ftp on page 3711](#)
- [execute switch-controller switch-software upload tftp on page 3712](#)
- [execute switch-controller virtual-port-pool request on page 3712](#)
- [execute switch-controller virtual-port-pool return on page 3712](#)
- [execute switch-controller virtual-port-pool show on page 3713](#)
- [execute switch-controller virtual-port-pool show-by-pool on page 3713](#)
- [execute switch-controller virtual-port-pool show-by-property on page 3713](#)
- [execute switch-controller virtual-port-pool show-by-tag on page 3713](#)

execute switch-controller custom-command

Push a FortiSwitch custom command to a FortiSwitch device.

```
execute switch-controller custom-command <cmd-name> <target-switch>
```

Parameter	Description	Type	Size
<cmd-name>	Names of commands to be pushed to this FortiSwitch device, as configured under config switch-controller custom-command.	string	
<target-switch>	FortiSwitch device to push the custom command to.	string	

execute switch-controller diagnose-connection

Get FortiSwitch connection diagnostics.

```
execute switch-controller diagnose-connection <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller diagnose-connection-v6

Get FortiSwitch IPv6 connection diagnostics.

```
execute switch-controller diagnose-connection-v6 <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller flapguard reset

Reset flapguard on port.

```
execute switch-controller flapguard reset <switch-name> <port>
```

Parameter	Description	Type	Size
<switch-name>	Name.	string	
<port>	FortiSwitch port.	string	

execute switch-controller get-conn-status

Get FortiSwitch connection status.

```
execute switch-controller get-conn-status <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller get-physical-conn dot

Get FortiLink connectivity graph in dot output format.

```
execute switch-controller get-physical-conn dot <fortilink-name>
```

Parameter	Description	Type	Size
<fortilink-name>	FortiLink name.	string	

execute switch-controller get-physical-conn standard

Get FortiLink connectivity graph in standard output format.

```
execute switch-controller get-physical-conn standard <fortilink-name>
```

Parameter	Description	Type	Size
<fortilink-name>	FortiLink name.	string	

execute switch-controller get-sync-status all

Get FortiSwitch sync status.

```
execute switch-controller get-sync-status all
```

execute switch-controller get-sync-status group

Get FortiSwitch sync status by group.

```
execute switch-controller get-sync-status group <group>
```

Parameter	Description	Type	Size
<group>	Group Name.	string	

execute switch-controller get-sync-status serial

Get FortiSwitch sync status by switch serial number.

```
execute switch-controller get-sync-status serial <switch-serial-number>
```

Parameter	Description	Type	Size
<switch-serial-number>	Serial Number.	string	

execute switch-controller get-sync-status switch-id

Get FortiSwitch sync status by switch.

```
execute switch-controller get-sync-status switch-id <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller get-upgrade-status

Get FortiSwitch upgrade status.

```
execute switch-controller get-upgrade-status
```

execute switch-controller ssh

SSH to FortiSwitch.

```
execute switch-controller ssh <user> <switch>
```

Parameter	Description	Type	Size
<user>	user.	string	
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action 802-1X clear-auth-mac

Clear FortiSwitch MAC entry.

```
execute switch-controller switch-action 802-1X clear-auth-mac <switch> <mac>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<mac>	MAC address.	string	

execute switch-controller switch-action 802-1X clear-auth-port

Clear FortiSwitch MAC entries on a single interface.

```
execute switch-controller switch-action 802-1X clear-auth-port <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	FortiSwitch port.	string	

execute switch-controller switch-action bpdu-guard reset

Reset BPDU guard on switch-interface.

```
execute switch-controller switch-action bpdu-guard reset <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	FortiSwitch port.	string	

execute switch-controller switch-action cable-diag

Run a TDR diagnostic test on the specified FortiSwitch port.

```
execute switch-controller switch-action cable-diag <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	FortiSwitch port.	string	

execute switch-controller switch-action factory-reset

Set FortiSwitch to factory default settings.

```
execute switch-controller switch-action factory-reset <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action flow-tracking delete-flows-all

Delete all flows in the FortiSwitch.

```
execute switch-controller switch-action flow-tracking delete-flows-all <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action flow-tracking expire-flows-all

Expire all flows in the FortiSwitch.

```
execute switch-controller switch-action flow-tracking expire-flows-all <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action igmp-snoop clear-learned

Clear FortiSwitch IGMP snooping multicast Groups and Queriers.

```
execute switch-controller switch-action igmp-snoop clear-learned <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action loop-guard reset

Reset loop-guard on switch-interface.

```
execute switch-controller switch-action loop-guard reset <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	FortiSwitch port.	string	

execute switch-controller switch-action mac-device-reset dynamic

Remove specific or all DPP devices.

```
execute switch-controller switch-action mac-device-reset dynamic <mac>
```

Parameter	Description	Type	Size
<mac>	MAC address of the DPP device.	string	

execute switch-controller switch-action mac-device-reset nac

Remove NAC devices and return MAC to onboarding VLAN.

```
execute switch-controller switch-action mac-device-reset nac <mac>
```

Parameter	Description	Type	Size
<mac>	MAC address of the NAC device.	string	

execute switch-controller switch-action mac-limit-violation reset all

Reset all MAC learning limit violations in FortiSwitch.

```
execute switch-controller switch-action mac-limit-violation reset all <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action mac-limit-violation reset interface

Reset MAC learning limit violations on a FortiSwitch interface.

```
execute switch-controller switch-action mac-limit-violation reset interface <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	FortiSwitch ports.	string	

execute switch-controller switch-action mac-limit-violation reset vlan

Reset MAC learning limit violations on a FortiSwitch VLAN.

```
execute switch-controller switch-action mac-limit-violation reset vlan <switch> <vlan-id>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<vlan-id>	FortiSwitch VLAN ID.	string	

execute switch-controller switch-action mclag stats clear icl

Clears MCLAG inter-chassis-link statistics.

```
execute switch-controller switch-action mclag stats clear icl <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action mclag stats clear mlag

Clears MCLAGs statistics for MCLAG enabled trunk.


```
execute switch-controller switch-action mclag stats clear mlag <switch> <mclag-trunk-name>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<mclag-trunk-name>	MCLAG's trunk name.	string	

execute switch-controller switch-action physical-ports led-flash switch-group

Enable LED flash mode on FortiSwitches in the switch-group.

```
execute switch-controller switch-action physical-ports led-flash switch-group <switch-group ID> <time>
```

Parameter	Description	Type	Size
<switch-group ID>	FortiSwitch group ID.	string	
<time>	FortiSwitch LED flash mode in minutes < disable 5 15 30 60 >.	string	

execute switch-controller switch-action physical-ports led-flash switch-id

Enable FortiSwitch LED flash mode by switch name.

```
execute switch-controller switch-action physical-ports led-flash switch-id <switch> <time>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<time>	FortiSwitch LED flash mode in minutes < disable 5 15 30 60 >.	string	

execute switch-controller switch-action physical-ports led-flash tier1

Enable LED flash mode on all tier 1 FortiSwitch units.

```
execute switch-controller switch-action physical-ports led-flash tier1 <time>
```

Parameter	Description	Type	Size
<time>	FortiSwitch LED flash mode in minutes < disable 5 15 30 60 >.	string	

execute switch-controller switch-action physical-ports led-flash tier2plus

Enable LED flash mode on all tier 2 and lower FortiSwitch units.

```
execute switch-controller switch-action physical-ports led-flash tier2plus <time>
```

Parameter	Description	Type	Size
<time>	FortiSwitch LED flash mode in minutes < disable 5 15 30 60 >.	string	

execute switch-controller switch-action poe reset

Reset PoE port on FortiSwitch.

```
execute switch-controller switch-action poe reset <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	FortiSwitch port.	string	

execute switch-controller switch-action restart delay all

Restart delay all FortiSwitch devices.

```
execute switch-controller switch-action restart delay all
```

execute switch-controller switch-action restart delay switch-group

Restart delay FortiSwitch devices belonging to switch-group.

```
execute switch-controller switch-action restart delay switch-group <switch-group ID>
```

Parameter	Description	Type	Size
<switch-group ID>	Switch group ID.	string	

execute switch-controller switch-action restart delay switch-id

Restart delay FortiSwitch device identified by switch name.

```
execute switch-controller switch-action restart delay switch-id <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action restart swtp all

Restart all FortiSwitch devices.

```
execute switch-controller switch-action restart swtp all
```

execute switch-controller switch-action restart swtp switch-group

Restart FortiSwitch devices belonging to switch-group.

```
execute switch-controller switch-action restart swtp switch-group <switch-group ID>
```

Parameter	Description	Type	Size
<switch-group ID>	Switch group ID.	string	

execute switch-controller switch-action restart swtp switch-id

Restart FortiSwitch device identified by switch name.

```
execute switch-controller switch-action restart swtp switch-id <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action set-standalone

Set FortiSwitch to local/non-FortiLink mode.

```
execute switch-controller switch-action set-standalone <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action sticky-mac delete-unsaved all

Delete all unsync Sticky MAC entries on FSW.

```
execute switch-controller switch-action sticky-mac delete-unsaved all <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action sticky-mac delete-unsaved interface

Delete specific interface's unsync Sticky MAC entries on FSW.

```
execute switch-controller switch-action sticky-mac delete-unsaved interface <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	Delete unsaved Sticky MAC entries for the specified interface.	string	

execute switch-controller switch-action sticky-mac save all

Sync and save all Sticky MAC entries to config file (loads entries on boot).

```
execute switch-controller switch-action sticky-mac save all <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-action sticky-mac save interface

Sync and save specific interface Sticky MAC entries to config file (loads entries on boot).

```
execute switch-controller switch-action sticky-mac save interface <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	Save Sticky MAC entries for the specified interface.	string	

execute switch-controller switch-software cancel all

Cancel staged image to all FortiSwitch devices.

```
execute switch-controller switch-software cancel all
```

execute switch-controller switch-software cancel switch-group

Cancel staged image to FortiSwitch devices belonging to switch-group.

```
execute switch-controller switch-software cancel switch-group <switch-group ID>
```

Parameter	Description	Type	Size
<switch-group ID>	Switch group ID.	string	

execute switch-controller switch-software cancel switch-id

Cancel staged image to FortiSwitch device identified by switch name.

```
execute switch-controller switch-software cancel switch-id <switch>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	

execute switch-controller switch-software delete

Delete FortiSwitch image.

```
execute switch-controller switch-software delete <all>|<image-name>
```

Parameter	Description	Type	Size
<all> <image-name>	Delete all images or specific image.	string	

execute switch-controller switch-software list-available

List FortiSwitch image(s) available on FortiGate.

```
execute switch-controller switch-software list-available
```

execute switch-controller switch-software stage all

Stage image to all FortiSwitch devices.

```
execute switch-controller switch-software stage all <filename>
```

Parameter	Description	Type	Size
<filename>	FortiSwitch image filename.	string	

execute switch-controller switch-software stage switch-group

Stage image to FortiSwitch devices belonging to switch-group.

```
execute switch-controller switch-software stage switch-group <switch-group ID> <filename>
```

Parameter	Description	Type	Size
<switch-group ID>	Switch group ID.	string	
<filename>	FortiSwitch image filename.	string	

execute switch-controller switch-software stage switch-id

Stage image to FortiSwitch device identified by switch name.

```
execute switch-controller switch-software stage switch-id <switch> <filename>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<filename>	FortiSwitch image filename.	string	

execute switch-controller switch-software upgrade

Upgrade FortiSwitch image to a managed FortiSwitch device.

```
execute switch-controller switch-software upgrade <switch> <filename>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<filename>	FortiSwitch image filename.	string	

execute switch-controller switch-software upload ftp

Upload a FortiSwitch image from FTP server.

```
execute switch-controller switch-software upload ftp <string> <ftp server>[:ftp port]  
<Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	FortiSwitch image name on the FTP server.	string	

Parameter	Description	Type	Size
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute switch-controller switch-software upload tftp

Upload a FortiSwitch image from TFTP server.

```
execute switch-controller switch-software upload tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	FortiSwitch image name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute switch-controller virtual-port-pool request

Request virtual port from pool.

```
execute switch-controller virtual-port-pool request <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	FortiSwitch port.	string	

execute switch-controller virtual-port-pool return

Return virtual port to pool.

```
execute switch-controller virtual-port-pool return <switch> <port>
```

Parameter	Description	Type	Size
<switch>	FortiSwitch device ID.	string	
<port>	FortiSwitch port.	string	

execute switch-controller virtual-port-pool show

Show details of virtual ports in pool.

```
execute switch-controller virtual-port-pool show
```

execute switch-controller virtual-port-pool show-by-pool

Show details of virtual ports in pool by pool name.

```
execute switch-controller virtual-port-pool show-by-pool <pool>
```

Parameter	Description	Type	Size
<pool>	Pool Name.	string	

execute switch-controller virtual-port-pool show-by-property

Show details of virtual ports in pool by property name.

```
execute switch-controller virtual-port-pool show-by-property <property>
```

Parameter	Description	Type	Size
<property>	Property Name.	string	

execute switch-controller virtual-port-pool show-by-tag

Show details of virtual ports in pool by tag name.

```
execute switch-controller virtual-port-pool show-by-tag <tag>
```

Parameter	Description	Type	Size
<tag>	Tag Name.	string	

execute sync-IPSec

Sync all IPSec from peers.

```
execute sync-IPSec
```

execute sync-session

Sync all sessions from peers.

```
execute sync-session
```

execute system

system

This topic includes the following commands:

- [execute system custom-language import on page 3714](#)
- [execute system fortisandbox test-connectivity on page 3714](#)

execute system custom-language import

Import a custom language from the TFTP server.

```
execute system custom-language import <string> <string> <ip>
```

Parameter	Description	Type	Size
<string>	The language name.	string	
<string>	The file name on the TFTP server.	string	
<ip>	IP address of the TFTP server.	string	

execute system fortisandbox test-connectivity

Query FortiSandbox connection status.

```
execute system fortisandbox test-connectivity
```

execute tac

tac

This topic includes the following commands:

- [execute tac report on page 3715](#)

execute tac report

Debug report.

```
execute tac report
```

execute telnet

Simple telnet client.

```
execute telnet <dest> <port>
```

Parameter	Description	Type	Size
<dest>	IP address or domain name.	string	
<port>	port	string	

execute telnet-options

telnet-options

This topic includes the following commands:

- [execute telnet-options interface on page 3715](#)
- [execute telnet-options reset on page 3716](#)
- [execute telnet-options source on page 3716](#)
- [execute telnet-options view-settings on page 3716](#)

execute telnet-options interface

Auto | <outgoing interface>.

```
execute telnet-options interface <string>
```

Parameter	Description	Type	Size
<string>	Auto <outgoing interface>.	string	

execute telnet-options reset

Reset settings.

```
execute telnet-options reset
```

execute telnet-options source

Auto | <source interface IP>.

```
execute telnet-options source <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	<source interface IP> Auto	string	

execute telnet-options view-settings

View the current settings for TELNET option.

```
execute telnet-options view-settings
```

execute test

test

This topic includes the following commands:

- [execute test tftp-analytics-report on page 3716](#)

execute test tftp-analytics-report

tftp analytics report.

```
execute test tftp-analytics-report <ip> <dir> <checksum>
```

Parameter	Description	Type	Size
<ip>	IP address of the TFTP server.	string	
<dir>	Directory for the analytics report.	string	
<checksum>	Checksum for the analytics report.	string	

execute time

System time.

```
execute time <hh:mm:ss>
```

Parameter	Description	Type	Size
<hh:mm:ss>	hh: 0-23, mm: 0-59, ss: 0-59.	string	

execute traceroute

Traceroute {IP|hostname}.

```
execute traceroute <dest>
```

Parameter	Description	Type	Size
<dest>	IP address or hostname.	string	

execute traceroute-options

traceroute-options

This topic includes the following commands:

- [execute traceroute-options device on page 3718](#)
- [execute traceroute-options queries on page 3718](#)
- [execute traceroute-options reset on page 3718](#)
- [execute traceroute-options source on page 3718](#)
- [execute traceroute-options use-sdwan on page 3718](#)
- [execute traceroute-options view-settings on page 3719](#)
- [execute traceroute-options vrf on page 3719](#)

execute traceroute-options device

Auto | <iface>.

```
execute traceroute-options device <string>
```

Parameter	Description	Type	Size
<string>	Auto <iface>	string	

execute traceroute-options queries

Integer value to specify number of queries per hop.

```
execute traceroute-options queries <integer>
```

Parameter	Description	Type	Size
<integer>	Integer value [1, 10].	string	

execute traceroute-options reset

Reset settings.

```
execute traceroute-options reset
```

execute traceroute-options source

Auto | <source interface IP>.

```
execute traceroute-options source <string>
```

Parameter	Description	Type	Size
<string>	Auto <source interface IP>.	string	

execute traceroute-options use-sdwan

Use SD-WAN rules to get output interface <yes | no>.

```
execute traceroute-options use-sdwan <string>
```

Parameter	Description	Type	Size
<string>	<yes no>.	string	

execute traceroute-options view-settings

View the current options of traceroute.

```
execute traceroute-options view-settings
```

execute traceroute-options vrf

VRF ID.

```
execute traceroute-options vrf <integer>
```

Parameter	Description	Type	Size
<integer>	<0-511>	string	

execute tracert6

Traceroute for IPv6.

```
execute tracert6
```

execute update-av

Update AV engine/definitions.

```
execute update-av
```

execute update-eip

Update external IP.

```
execute update-eip
```

execute update-external-resource

Download external resource.

```
execute update-external-resource <name>
```

Parameter	Description	Type	Size
<name>	External resource name	string	

execute update-ffdb-on-demand

Update ondemand FFDB from FDS.

```
execute update-ffdb-on-demand
```

execute update-geo-ip

Update IP Geography DB.

```
execute update-geo-ip
```

execute update-ips

Update IPS engine/definitions.

```
execute update-ips
```

execute update-now

Update now.


```
execute update-now
```

execute update-src-vis

Update src-vis object.

```
execute update-src-vis
```

execute upd-vd-license

Update VDOM license.

```
execute upd-vd-license <license key>
```

Parameter	Description	Type	Size
<license key>	VDOM license key.	string	

execute upload

upload

This topic includes the following commands:

- [execute upload config ftp on page 3721](#)
- [execute upload config tftp on page 3722](#)
- [execute upload image ftp on page 3722](#)
- [execute upload image tftp on page 3723](#)
- [execute upload report-img ftp on page 3723](#)
- [execute upload report-img tftp on page 3723](#)

execute upload config ftp

Load config file from FTP server.

```
execute upload config ftp <string> <comment> <ftp server>[:ftp port] <Enter>|<user> <passwd>  
<Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Configure file name(path) on the remote server.	string	
<comment>	comments	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter> <passwd>	Password may be needed to restore.	string	

execute upload config tftp

Load config from TFTP server to local disk.

```
execute upload config tftp <string> <comment> <tftp server>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<comment>	comments	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute upload image ftp

Load image from FTP server.

```
execute upload image ftp <string> <comment> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	Image file name(path) on the remote server.	string	
<comment>	comments	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute upload image tftp

Load image from TFTP server to local disk.

```
execute upload image tftp <string> <comment> <tftp server>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<comment>	comments	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute upload report-img ftp

upload report image file from ftp server

```
execute upload report-img ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd> <Enter>
```

Parameter	Description	Type	Size
<string>	Image file name(path) on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	
<Enter>		string	

execute upload report-img tftp

upload report image file from tftp server

```
execute upload report-img tftp <string> <tftp server> <Enter>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<Enter>		string	

execute vm-license

Download VM license from FortiCare.

```
execute vm-license <token> <proxy>
```

Parameter	Description	Type	Size
<token>	VM License Token.	string	
<proxy>	HTTP Proxy URL.	string	

execute vm-license-options

vm-license-options

This topic includes the following commands:

- [execute vm-license-options account-id on page 3724](#)
- [execute vm-license-options account-password on page 3724](#)
- [execute vm-license-options count on page 3725](#)
- [execute vm-license-options government on page 3725](#)
- [execute vm-license-options interval on page 3725](#)
- [execute vm-license-options proxy on page 3725](#)
- [execute vm-license-options reset on page 3726](#)
- [execute vm-license-options show on page 3726](#)
- [execute vm-license-options token on page 3726](#)

execute vm-license-options account-id

Account ID.

```
execute vm-license-options account-id <string>
```

Parameter	Description	Type	Size
<string>	Account ID.	string	

execute vm-license-options account-password

Account password.

```
execute vm-license-options account-password <string>
```

Parameter	Description	Type	Size
<string>	Account password.	string	

execute vm-license-options count

FortiFlex license download count (default=1, 0 means infinite).

```
execute vm-license-options count <integer>
```

Parameter	Description	Type	Size
<integer>	API call count.	string	

execute vm-license-options government

For government use <yes | no>.

```
execute vm-license-options government <string>
```

Parameter	Description	Type	Size
<string>	<yes no>.	string	

execute vm-license-options interval

FortiFlex license download interval (1-3600 sec, default=60).

```
execute vm-license-options interval <integer>
```

Parameter	Description	Type	Size
<integer>	API call interval.	string	

execute vm-license-options proxy

HTTP proxy URL.

```
execute vm-license-options proxy <string>
```

Parameter	Description	Type	Size
<string>	HTTP proxy URL.	string	

execute vm-license-options reset

Reset options.

```
execute vm-license-options reset
```

execute vm-license-options show

Show options.

```
execute vm-license-options show
```

execute vm-license-options token

Token.

```
execute vm-license-options token <string>
```

Parameter	Description	Type	Size
<string>	Token.	string	

execute vpn

vpn

This topic includes the following commands:

- [execute vpn certificate ca export tftp on page 3727](#)
- [execute vpn certificate ca import auto on page 3727](#)
- [execute vpn certificate ca import bundle on page 3728](#)
- [execute vpn certificate ca import est on page 3728](#)
- [execute vpn certificate ca import tftp on page 3729](#)
- [execute vpn certificate crl import auto on page 3729](#)
- [execute vpn certificate ems_ca import tftp on page 3729](#)
- [execute vpn certificate hsm-local gch-get-versions on page 3729](#)
- [execute vpn certificate hsm-local status on page 3730](#)

- [execute vpn certificate hsm-local verify on page 3730](#)
- [execute vpn certificate local export tftp on page 3730](#)
- [execute vpn certificate local generate cmp-ec on page 3730](#)
- [execute vpn certificate local generate cmp-rsa on page 3731](#)
- [execute vpn certificate local generate default-gui-mgmt-cert on page 3732](#)
- [execute vpn certificate local generate default-ssl-ca on page 3732](#)
- [execute vpn certificate local generate default-ssl-ca-untrusted on page 3732](#)
- [execute vpn certificate local generate default-ssl-key-certs on page 3732](#)
- [execute vpn certificate local generate default-ssl-serv-key on page 3733](#)
- [execute vpn certificate local generate ec on page 3733](#)
- [execute vpn certificate local generate est on page 3734](#)
- [execute vpn certificate local generate rsa on page 3734](#)
- [execute vpn certificate local import tftp on page 3735](#)
- [execute vpn certificate local verify on page 3735](#)
- [execute vpn certificate remote export tftp on page 3736](#)
- [execute vpn certificate remote import tftp on page 3736](#)
- [execute vpn ikecrypt dhperf compute on page 3736](#)
- [execute vpn ikecrypt dhperf generate on page 3737](#)
- [execute vpn ipsec tunnel down on page 3737](#)
- [execute vpn ipsec tunnel up on page 3737](#)
- [execute vpn sslvpn del-all on page 3737](#)
- [execute vpn sslvpn del-tunnel on page 3738](#)
- [execute vpn sslvpn del-web on page 3738](#)
- [execute vpn sslvpn list on page 3738](#)

execute vpn certificate ca export tftp

Export CA certificate to a TFTP server.

```
execute vpn certificate ca export tftp <string> <string> <ip>
```

Parameter	Description	Type	Size
<string>	CA certificate name.	string	
<string>	File name on the TFTP server.	string	
<ip>	IP address of TFTP server.	string	

execute vpn certificate ca import auto

Import CA certificate via SCEP.

```
execute vpn certificate ca import auto <string> <string> <ip> <fingerprint>
```

Parameter	Description	Type	Size
<string>	URL of the CA server.	string	
<string>	CA Identifier (optional).	string	
<ip>	Source-IP for communications to the CA server (optional).	string	
<fingerprint>	Fingerprint for authenticating CA certificate from server (optional).	string	

execute vpn certificate ca import bundle

Import certificate bundle from a TFTP server.

```
execute vpn certificate ca import bundle <string> <ip>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<ip>	IP address of TFTP server.	string	

execute vpn certificate ca import est

Import CA certificate via EST.

```
execute vpn certificate ca import est <string> <string> <string> <string> <ip> <string> <string>  
<string> <string>
```

Parameter	Description	Type	Size
<string>	URL of the CA server. (e.g. https://example.com:1234).	string	
<string>	CA Identifier (optional).	string	
<string>	Verify CA server using this certificate (optional).	string	
<string>	Client certificate (optional).	string	
<ip>	Source-IP for communications to the CA server (optional).	string	
<string>	TLS-SRP Username (optional).	string	
<string>	TLS-SRP Password (optional).	string	
<string>	HTTP Authentication Username (optional).	string	
<string>	HTTP Authentication Password (optional).	string	

execute vpn certificate ca import tftp

Import CA certificate from a TFTP server.

```
execute vpn certificate ca import tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute vpn certificate crl import auto

Update CRL.

```
execute vpn certificate crl import auto <string>
```

Parameter	Description	Type	Size
<string>	CRL name.	string	

execute vpn certificate ems_ca import tftp

Import Testing EMS CA certificate from a TFTP server.

```
execute vpn certificate ems_ca import tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute vpn certificate hsm-local gch-get-versions

List available crypto-key-versions.

```
execute vpn certificate hsm-local gch-get-versions <string> <string>
```

Parameter	Description	Type	Size
<string>	hsm-local certificate name.	string	
<string>	Access token or JSON Web Token to be used as bearer token in request.	string	

execute vpn certificate hsm-local status

Status check for an hsm-local certificate.

```
execute vpn certificate hsm-local status <string> <string>
```

Parameter	Description	Type	Size
<string>	hsm-local certificate name.	string	
<string>	Access token or JSON Web Token to be used as bearer token in request.	string	

execute vpn certificate hsm-local verify

Verify between hsm-local certificate and its private key.

```
execute vpn certificate hsm-local verify <string> <string>
```

Parameter	Description	Type	Size
<string>	hsm-local certificate name.	string	
<string>	Access token or JSON Web Token to be used as bearer token in request.	string	

execute vpn certificate local export tftp

Export local certificate or certificate request to a TFTP server.

```
execute vpn certificate local export tftp <string> <string> <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	
<string>	Certificate file type ('cer' 'p12' 'csr').	string	
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute vpn certificate local generate cmp-ec

Generate a ECDSA certificate request over CMPv2.

```
execute vpn certificate local generate cmp-ec <string> <string> <string> <string> <string>
<string> <string> <string> <string> <string> <ip>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	
<string>	Elliptic curve name: secp256r1, secp384r1 and secp521r1.	string	
<string>	Server ('ADDRESS:PORT' for CMP server).	string	
<string>	Path (Path location inside CMP server)	string	
<string>	SrvCert (CMDB name of CMP server's certificate/root-CA)	string	
<string>	AuthCert (CMDB name of client's current certificate)	string	
<string>	User (Username for doing the IR with a pre-shared key)	string	
<string>	Password (Password for doing the IR with a pre-shared key)	string	
<string>	Subject (optional, e.g. "CN=User,O=Org,OU=Unit").	string	
<string>	Subject alternative name (optional, e.g. "DNS:dns1.com,IP:192.168.1.99").	string	
<ip>	Source-IP for communications to the CMP server (optional).	string	

execute vpn certificate local generate cmp-rsa

Generate a RSA certificate request over CMPv2.

```
execute vpn certificate local generate cmp-rsa <string> <number> <string> <string> <string>
<string> <string> <string> <string> <string> <ip>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	
<number>	Key size: 1024, 1536, 2048, 4096.	string	
<string>	Server ('ADDRESS:PORT' for CMP server, add 'https://' before address to enable ssl/tls).	string	
<string>	Path (Path location inside CMP server)	string	
<string>	SrvCert (CMDB name of CMP server's certificate/root-CA)	string	
<string>	AuthCert (CMDB name of client's current certificate)	string	
<string>	User (Username for doing the IR with a pre-shared key)	string	

Parameter	Description	Type	Size
<string>	Password (Password for doing the IR with a pre-shared key)	string	
<string>	Subject (optional, e.g. "CN=User,O=Org,OU=Unit").	string	
<string>	Subject alternative name (optional, e.g. "DNS:dns1.com,IP:192.168.1.99").	string	
<ip>	Source-IP for communications to the CMP server (optional).	string	

execute vpn certificate local generate default-gui-mgmt-cert

Generate the default GUI mgmt admin-server certificate.

```
execute vpn certificate local generate default-gui-mgmt-cert
```

execute vpn certificate local generate default-ssl-ca

Generate the default CA certificate used by SSL Inspection.

```
execute vpn certificate local generate default-ssl-ca
```

execute vpn certificate local generate default-ssl-ca-untrusted

Generate the default untrusted CA certificate used by SSL Inspection.

```
execute vpn certificate local generate default-ssl-ca-untrusted
```

execute vpn certificate local generate default-ssl-key-certs

Generate the default RSA, DSA and ECDSA key certs for ssl resign.

```
execute vpn certificate local generate default-ssl-key-certs
```

execute vpn certificate local generate default-ssl-serv-key

Generate the default server key used by SSL Inspection.

```
execute vpn certificate local generate default-ssl-serv-key
```

execute vpn certificate local generate ec

Generate an elliptic curve certificate request.

```
execute vpn certificate local generate ec <string> <string> <string> <string> <string> <string>
<string> <string> <string> <string> <string> <string> <ip> <string> <string> <string> <string>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	
<string>	Elliptic curve name: secp256r1, secp384r1 and secp521r1.	string	
<string>	Subject (Host IP/Domain Name/E-Mail).	string	
<string>	Country name (e.g. Canada) or country code (e.g. ca).	string	
<string>	State.	string	
<string>	City.	string	
<string>	Org.	string	
<string>	Unit(s); ',' as delimiter.	string	
<string>	Email.	string	
<string>	Subject alternative name (optional).	string	
<string>	URL of the CA server for signing via SCEP (optional).	string	
<string>	Challenge password for signing via SCEP (optional).	string	
<ip>	Source-IP for communications to the CA server (optional).	string	
<string>	CA identifier of the CA server for signing via SCEP (optional).	string	
<string>	Password for private-key (optional).	string	
<string>	Installed CA certificate for generating fingerprint for validating CA from SCEP server (optional).	string	
<string>	Fingerprint for authenticating CA certificate from SCEP server. Ignored if valid CA for generating fingerprint is specified (optional).	string	

execute vpn certificate local generate est

Generate an certificate via Enrollment over Secure Transport.

```
execute vpn certificate local generate est <string> <string> <string> <string> <string> <string>
<string> <string> <string> <string> <string> <ip> <string> <string>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	
<string>	Cryptography algorithm: rsa-1024, rsa-1536, rsa-2048, rsa-4096, ec-secp256r1, ec-secp384r1, ec-secp521r1	string	
<string>	URL of the CA server. (e.g. https://example.com:1234).	string	
<string>	Subject (optional, e.g. "CN=User,O=Org,OU=Unit").	string	
<string>	Subject alternative name (optional, e.g. "DNS:dns1.com,IP:192.168.1.99").	string	
<string>	HTTP Authentication Username (optional).	string	
<string>	HTTP Authentication Password (optional).	string	
<string>	CA Identifier (optional).	string	
<string>	CA Server certificate (optional).	string	
<string>	Password for private-key (optional).	string	
<string>	Client certificate (optional).	string	
<ip>	Source-IP for communications to the CA server (optional).	string	
<string>	TLS-SRP Username (optional).	string	
<string>	TLS-SRP Password (optional).	string	

execute vpn certificate local generate rsa

Generate a RSA certificate request.

```
execute vpn certificate local generate rsa <string> <number> <string> <string> <string> <string>
<string> <string> <string> <string> <string> <string> <ip> <string> <string> <string> <string>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	
<number>	Key size: 1024, 1536, 2048, 4096.	string	
<string>	Subject (Host IP/Domain Name/E-Mail).	string	

Parameter	Description	Type	Size
<string>	Country name (e.g. Canada) or country code (e.g. ca).	string	
<string>	State.	string	
<string>	City.	string	
<string>	Org.	string	
<string>	Unit(s); ',' as delimiter.	string	
<string>	Email.	string	
<string>	Subject alternative name (optional).	string	
<string>	URL of the CA server for signing via SCEP (optional).	string	
<string>	Challenge password for signing via SCEP (optional).	string	
<ip>	Source-IP for communications to the CA server (optional).	string	
<string>	CA identifier of the CA server for signing via SCEP (optional).	string	
<string>	Password for private-key (optional).	string	
<string>	Installed CA certificate for generating fingerprint for validating CA from SCEP server (optional).	string	
<string>	Fingerprint for authenticating CA certificate from SCEP server. Ignored if valid CA for generating fingerprint is specified (optional).	string	

execute vpn certificate local import tftp

Import the signed certificate from a TFTP server.

```
execute vpn certificate local import tftp <string> <tftp server> <string> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	
<string>	Certificate file type ('cer' 'p12').	string	
<Enter> <passwd>	Password for PKCS12 file.	string	

execute vpn certificate local verify

Verify certificate and private key files match and regenerate if mismatched.

```
execute vpn certificate local verify <string>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	

execute vpn certificate remote export tftp

Export REMOTE certificate to a TFTP server.

```
execute vpn certificate remote export tftp <string> <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	REMOTE certificate name.	string	
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute vpn certificate remote import tftp

Import REMOTE certificate from a TFTP server.

```
execute vpn certificate remote import tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute vpn ikecrypt dhperf compute

Run DH generate and compute benchmark.

```
execute vpn ikecrypt dhperf compute <rounds>
```

Parameter	Description	Type	Size
<rounds>	Number of DH generate and compute rounds to perform per group <1-100000>.	string	

execute vpn ikecrypt dhperf generate

Run DH generate benchmark.

```
execute vpn ikecrypt dhperf generate <rounds>
```

Parameter	Description	Type	Size
<rounds>	Number of DH generate rounds to perform per group <1-100000>.	string	

execute vpn ipsec tunnel down

Shut down the specified IPsec tunnel.

```
execute vpn ipsec tunnel down <phase2> <phase1> <serial>
```

Parameter	Description	Type	Size
<phase2>	Phase2 name.	string	
<phase1>	Phase1 name.	string	
<serial>	Phase2 serial number.	string	

execute vpn ipsec tunnel up

Activate the specified IPsec tunnel.

```
execute vpn ipsec tunnel up <phase2> <phase1> <serial>
```

Parameter	Description	Type	Size
<phase2>	Phase2 name.	string	
<phase1>	Phase1 name.	string	
<serial>	Phase2 serial number.	string	

execute vpn sslvpn del-all

Delete all connections under current VDOM.

```
execute vpn sslvpn del-all <tunnel>
```

Parameter	Description	Type	Size
<tunnel>	Press <Enter> to delete all or type "tunnel" to delete session only.	string	

execute vpn sslvpn del-tunnel

Delete session connection.

```
execute vpn sslvpn del-tunnel <index>
```

Parameter	Description	Type	Size
<index>	Session index.	string	

execute vpn sslvpn del-web

Delete web connection.

```
execute vpn sslvpn del-web <index>
```

Parameter	Description	Type	Size
<index>	Web index.	string	

execute vpn sslvpn list

List connections.

```
execute vpn sslvpn list <web|tunnel>
```

Parameter	Description	Type	Size
<web tunnel>	Web or session.	string	

execute wake-on-lan

Wake On LAN command.

```
execute wake-on-lan <interface> <host-mac> <protocol> <port> <ip> <password>
```

Parameter	Description	Type	Size
<interface>	Network interface to send out WoL packets.	string	
<host-mac>	Host MAC address to be woken up.	string	
<protocol>	Protocol used by WoL packets (1-WoL, 2-UDP, default = 2).	string	
<port>	Port used by UDP WoL packets, (0, 7, or 9, default = 9).	string	
<ip>	Broadcast IP used by UDP WoL packets.	string	
<password>	Password of the destination host if SecureOn is enabled.	string	

execute webcache

webcache

This topic includes the following commands:

- [execute webcache delete regular-expression on page 3739](#)
- [execute webcache delete simple-string on page 3739](#)
- [execute webcache delete status on page 3740](#)
- [execute webcache delete wildcard on page 3740](#)

execute webcache delete regular-expression

Delete objects matching a regular expression in webcache.

```
execute webcache delete regular-expression <pattern>
```

Parameter	Description	Type	Size
<pattern>	Pattern.	string	

execute webcache delete simple-string

Delete objects matching a simple string in webcache.

```
execute webcache delete simple-string <pattern>
```

Parameter	Description	Type	Size
<pattern>	Pattern.	string	

execute webcache delete status

Query pattern deletion status.

```
execute webcache delete status
```

execute webcache delete wildcard

Delete objects matching a wildcard in webcache.

```
execute webcache delete wildcard <pattern>
```

Parameter	Description	Type	Size
<pattern>	Pattern.	string	

execute webfilter

webfilter

This topic includes the following commands:

- [execute webfilter quota-reset on page 3740](#)

execute webfilter quota-reset

Reset the WF quota for a given user.

```
execute webfilter quota-reset <wf-profile> <endpoint>
```

Parameter	Description	Type	Size
<wf-profile>	Web filter profile.	string	
<endpoint>	Authenticated user or IP address.	string	

execute wireless-controller

wireless-controller

This topic includes the following commands:

- [execute wireless-controller create-sae-pk on page 3741](#)
- [execute wireless-controller delete-wtp-image on page 3741](#)
- [execute wireless-controller hs20-icon backup-icon ftp on page 3742](#)
- [execute wireless-controller hs20-icon backup-icon tftp on page 3742](#)
- [execute wireless-controller hs20-icon delete-hs-icon on page 3742](#)
- [execute wireless-controller hs20-icon list-hs-icon on page 3742](#)
- [execute wireless-controller hs20-icon upload-icon ftp on page 3743](#)
- [execute wireless-controller hs20-icon upload-icon tftp on page 3743](#)
- [execute wireless-controller led-blink on page 3743](#)
- [execute wireless-controller list-wtp-image on page 3743](#)
- [execute wireless-controller mpsk-key create-keys on page 3744](#)
- [execute wireless-controller push-wtp-image on page 3744](#)
- [execute wireless-controller reset-wtp on page 3744](#)
- [execute wireless-controller restart-acd on page 3745](#)
- [execute wireless-controller rolling-wtp-upgrade on page 3745](#)
- [execute wireless-controller spectral-scan on page 3745](#)
- [execute wireless-controller upload-wtp-image ftp on page 3745](#)
- [execute wireless-controller upload-wtp-image tftp on page 3746](#)

execute wireless-controller create-sae-pk

Create SAE PK keys.

```
execute wireless-controller create-sae-pk <string> <string>
```

Parameter	Description	Type	Size
<string>	SSID.	string	
<string>	Curve: prime256v1 secp384r1 secp521r1.	string	

execute wireless-controller delete-wtp-image

Delete WTP images.

```
execute wireless-controller delete-wtp-image <all>|<all-pushing>|<image-name>
```

Parameter	Description	Type	Size
<all> <all-pushing> <image-name>	Delete all images or specific image.	string	

execute wireless-controller hs20-icon backup-icon ftp

Backup a hotspot icon to FTP server.

```
execute wireless-controller hs20-icon backup-icon ftp <string> <ftp server>[:ftp port]  
<Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	Icon file name on AC.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute wireless-controller hs20-icon backup-icon tftp

Backup a hotspot icon to TFTP server.

```
execute wireless-controller hs20-icon backup-icon tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	Icon file name on AC.	string	
<tftp server>	IP/IPv6 or FQDN address of TFTP server.	string	

execute wireless-controller hs20-icon delete-hs-icon

Delete hotspot icons.

```
execute wireless-controller hs20-icon delete-hs-icon
```

execute wireless-controller hs20-icon list-hs-icon

List hotspot icons.

```
execute wireless-controller hs20-icon list-hs-icon
```

execute wireless-controller hs20-icon upload-icon ftp

Upload a hotspot icon from FTP server.

```
execute wireless-controller hs20-icon upload-icon ftp <string> <ftp server>[:ftp port]  
<Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	Icon file name on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute wireless-controller hs20-icon upload-icon tftp

Upload a hotspot icon from TFTP server.

```
execute wireless-controller hs20-icon upload-icon tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	Icon file name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

execute wireless-controller led-blink

Blink status LED or power LED of managed FortiAP.

```
execute wireless-controller led-blink <wtp-id> <mode> <duration>
```

Parameter	Description	Type	Size
<wtp-id>	WTP ID.	string	
<mode>	[on off]	string	
<duration>	Blink duration in seconds (0 = unlimited).	string	

execute wireless-controller list-wtp-image

List WTP images.

```
execute wireless-controller list-wtp-image
```

execute wireless-controller mpsk-key create-keys

Create random MPSK keys.

```
execute wireless-controller mpsk-key create-keys <string> <string> <string> <string> <int> <int>
```

Parameter	Description	Type	Size
<string>	VDOM.	string	
<string>	MPSK profile name.	string	
<string>	MPSK group name.	string	
<string>	Key prefix.	string	
<int>	Key count.	string	
<int>	Key length.	string	

execute wireless-controller push-wtp-image

Push WTP image to a managed WTP.

```
execute wireless-controller push-wtp-image <vdom> <wtp-id> <filename>
```

Parameter	Description	Type	Size
<vdom>	WTP session VDOM.	string	
<wtp-id>	WTP ID.	string	
<filename>	WTP image filename.	string	

execute wireless-controller reset-wtp

Restart managed WTP.

```
execute wireless-controller reset-wtp <all>|<SN>|<wtp-group>
```

Parameter	Description	Type	Size
<all> <SN> <wtp-group>	WTP serial number or WTP group.	string	

execute wireless-controller restart-acd

Restart wireless controller daemon.

```
execute wireless-controller restart-acd
```

execute wireless-controller rolling-wtp-upgrade

Rolling upgrade managed WTP.

```
execute wireless-controller rolling-wtp-upgrade <all>|<SN>|<wtp-group>
```

Parameter	Description	Type	Size
<all> <SN> <wtp-group>	WTP serial number or WTP group.	string	

execute wireless-controller spectral-scan

Enable/disable spectral scan.

```
execute wireless-controller spectral-scan <wtp-id> <radio-id> <mode> <duration> <channel> <report-interval>
```

Parameter	Description	Type	Size
<wtp-id>	WTP ID.	string	
<radio-id>	Radio ID	string	
<mode>	[on off scan-only keep-alive clear]	string	
<duration>	Spectrum scan duration in seconds (0 = unlimited).	string	
<channel>	Spectrum scan channels separated by commas. (0 or empty = all supported channels).	string	
<report-interval>	Time between two spectral reports from the AP in millisecond (<min> - <max>, 0 or empty = 1000ms).	string	

execute wireless-controller upload-wtp-image ftp

Upload a WTP image from FTP server.

```
execute wireless-controller upload-wtp-image ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	WTP image file name on the remote server.	string	
<ftp server>[:ftp port]	FTP server IPv4, IPv6, or FQDN can be attached with port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute wireless-controller upload-wtp-image tftp

Upload a WTP image from TFTP server.

```
execute wireless-controller upload-wtp-image tftp <string> <tftp server>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<tftp server>	TFTP server IPv4, IPv6, or FQDN.	string	

Included devices

This reference includes commands from the following FortiGate model:

- FortiGate-1000D
- FortiGate-1000F
- FortiGate-1001F
- FortiGate-100F
- FortiGate-101F
- FortiGate-1100E
- FortiGate-1101E
- FortiGate-120G
- FortiGate-121G
- FortiGate-1800F
- FortiGate-1801F
- FortiGate-2000E
- FortiGate-200E
- FortiGate-200F
- FortiGate-201E
- FortiGate-201F
- FortiGate-2200E
- FortiGate-2201E
- FortiGate-2500E
- FortiGate-2600F
- FortiGate-2601F
- FortiGate-3000D
- FortiGate-3000F
- FortiGate-3001F
- FortiGate-300E
- FortiGate-301E
- FortiGate-3100D
- FortiGate-3200D
- FortiGate-3200F
- FortiGate-3201F
- FortiGate-3300E
- FortiGate-3301E
- FortiGate-3400E
- FortiGate-3401E
- FortiGate-3500F
- FortiGate-3501F
- FortiGate-3600E
- FortiGate-3601E
- FortiGate-3700D
- FortiGate-3700F
- FortiGate-3701F
- FortiGate-3960E
- FortiGate-3980E
- FortiGate-400E-Bypass
- FortiGate-400E
- FortiGate-400F
- FortiGate-401E
- FortiGate-401F
- FortiGate-40F-3G4G
- FortiGate-40F
- FortiGate-4200F
- FortiGate-4201F
- FortiGate-4400F
- FortiGate-4401F
- FortiGate-5001E1
- FortiGate-5001E
- FortiGate-500E
- FortiGate-501E
- FortiGate-600E
- FortiGate-600F
- FortiGate-601E
- FortiGate-601F
- FortiGate-60F
- FortiGate-61F
- FortiGate-70F
- FortiGate-71F
- FortiGate-800D
- FortiGate-80F-Bypass
- FortiGate-80F-DSL
- FortiGate-80F-POE
- FortiGate-80F
- FortiGate-81F-POE
- FortiGate-81F
- FortiGate-900D
- FortiGate-900G
- FortiGate-901G
- FortiGate-90G
- FortiGate-91G
- FortiGate-VM64-Aliyun
- FortiGate-VM64-AWS
- FortiGate-VM64-Azure
- FortiGate-VM64-GCP
- FortiGate-VM64-OPC
- FortiGate-VM64
- FortiGateRugged-60F-3G4G
- FortiGateRugged-60F
- FortiGateRugged-70F-3G4G
- FortiGateRugged-70F
- FortiWiFi-40F-3G4G
- FortiWiFi-40F
- FortiWiFi-60F
- FortiWiFi-61F
- FortiWiFi-80F-2R-3G4G-DSL
- FortiWiFi-80F-2R
- FortiWiFi-81F-2R-3G4G-DSL
- FortiWiFi-81F-2R-3G4G-POE
- FortiWiFi-81F-2R-POE
- FortiWiFi-81F-2R



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.